

インターネットの

# 安全・安心 ハンドブック



内閣サイバーセキュリティセンター  
National center of Incident readiness and  
Strategy for Cybersecurity



サイバーセキュリティ普及啓発

協力



Ver 5.00





インターネットの

# 安全・安心 ハンドブック



内閣サイバーセキュリティセンター  
National center of Incident readiness and  
Strategy for Cybersecurity



サイバーセキュリティ普及啓発

協力



警察庁  
National Police Agency



総務省



経済産業省



独立行政法人  
情報処理推進機構

Ver 5.00





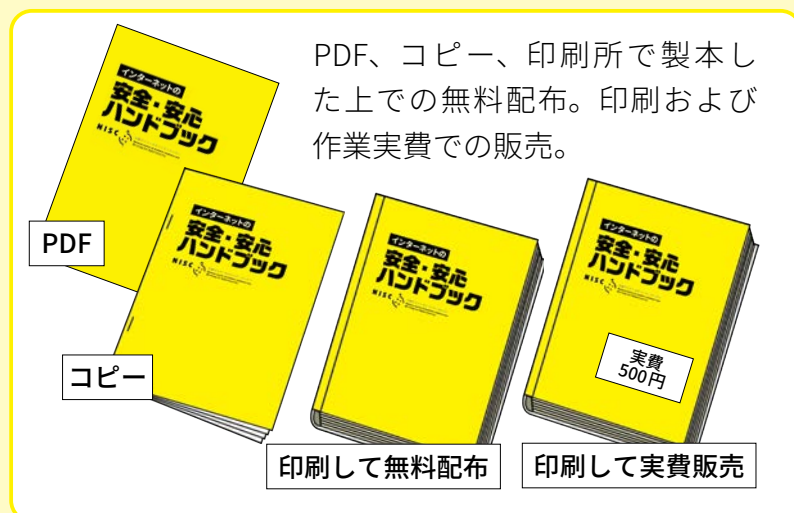
## 「インターネットの安全・安心ハンドブック」 は、下記のようにご利用いただけます。

本冊子の著作権は内閣サイバーセキュリティセンター(NISC)に留保されますが、内容に改変を加えないことを条件に、多様な形でご利用いただくことができます。

※製本用印刷データが必要な場合は下記までお問い合わせください

security\_awareness@cyber.go.jp

※合本やプリンタでの印刷にはNISCウェブサイト掲載のPDF版をお使いください



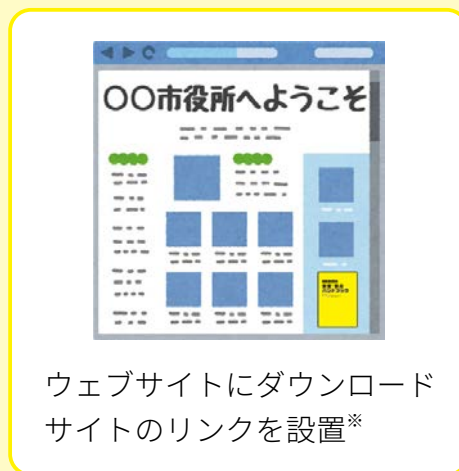
PDF、コピー、印刷所で製本した上での無料配布。印刷および作業実費での販売。



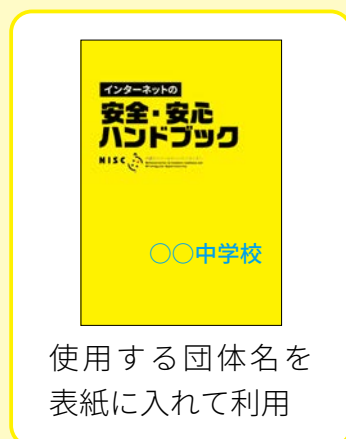
ページ単位、イラスト単位での利用、配布(ネット配布含む)



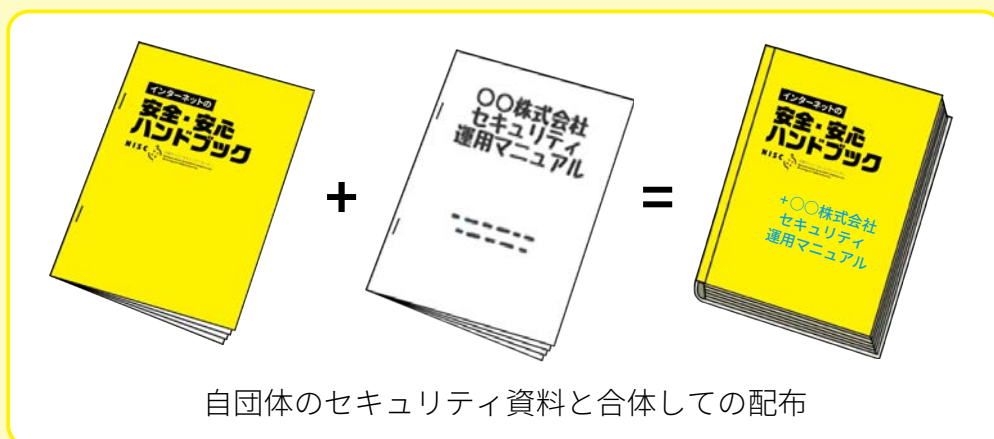
分割して配布、必要部分だけを抜粋して配布



ウェブサイトにダウンロードサイトのリンクを設置※



使用する団体名を表紙に入れて利用



自団体のセキュリティ資料と合体しての配布



# インターネットの安全・安心ハンドブック 活用法

## ■学校の授業で

「インターネットの安全・安心ハンドブック」は、中高生の方とその先生方に、セキュリティ意識を高めるための教材として使っていただけるように作成されています。

第1章で基礎的なセキュリティを固めつつ、サイバー攻撃による被害、SNSでのトラブルや情報モラルの重要性、スマホやパソコンを安全に利用するための設定、パスワード管理の大切さと通信の安全性を支える暗号化など、読む前に専門知識は必要なく学べます。

## ■ご家庭で

本書で解説しているセキュリティの考え方や守り方はご家庭にも役立ちます。

とくに第3章では、こどもがSNSを通してどんなトラブルや被害に遭う可能性があるのかを解説したり、こどもだけでなくシニアの方々を守るためのサービスなども解説したりしていますので、ご活用ください。

## ■中小組織で

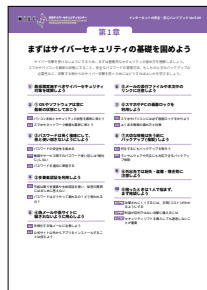
そして本書は中小企業や小さなNPO、一般社団法人などでも活用できます。

とくに第7章では、企業経営においてセキュリティ対策に投資すべき理由、企業だからこそ気を付けたいサイバー攻撃、テレワークを安全快適に利用するために必要なルール作り、最低限把握しておきたいセキュリティ関連の法律などを解説しています。

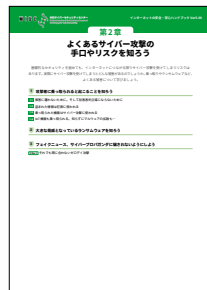
そして、付録ではセキュリティ部門担当者にも役立つガイダンスも紹介しています。

## 学校の授業で

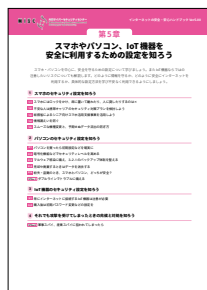
P.27「第1章 まずはサイバーセキュリティの基礎を固めよう」



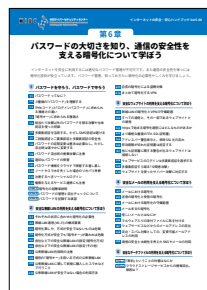
P.49「第2章 よくあるサイバー攻撃の手口やリスクを知ろう」



P.91「第5章 スマホやパソコン、IoT機器を安全に利用するための設定を知ろう」



P.109「第6章 パスワードの大切さを知り、通信の安全性を支える暗号化について学ぼう」



## ご家庭で

P.60「1.3 SNS やネットとの付き合い方の基本」

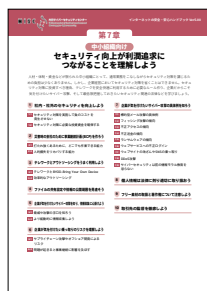


P.76「3.2 お年寄りを守る」

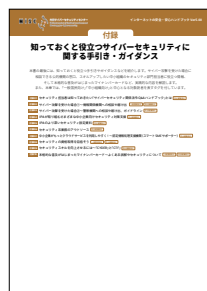


## 中小組織で

P.149「第7章 中小組織向け セキュリティ向上が利潤追求につながることを理解しよう」



P.173「付録 知っておくと役立つサイバーセキュリティに関する手引き・ガイダンス」



# 目次

インターネットの安全・安心ハンドブック 活用法	5
はじめに	10

## プロローグ インターネットにある基本的なリスクやトラブルを知ろう 13

1 サイバー攻撃とは？	14
2 ハッカーと攻撃者とは？	15
3 攻撃者が使う武器「マルウェア」とは？	16
3.1 どんな種類があるの？	16
3.2 どのような機能を持つものがあるの？	16
3.3 どんなものが感染したり、感染させたり、悪さをするようになるの？	17
4 サイバー攻撃の具体例は？	18
4.1 どんな攻撃があるのか？	18
4.2 会社や団体が狙われるとどうなる？	19
5 攻撃者とはどんな人物なの？	20
6 どうやって攻撃されるの？	21
6.1 おもにマルウェアなどを使って「技術的」に攻撃	21
6.2 人の心の隙を突く心理的な攻撃～ソーシャルエンジニアリング	22
7 SNSやネットのコミュニケーションで注意したいことは？	23
7.1 SNSやネット上の誹謗中傷対策	23
7.2 SNSやネット上の犯罪やトラブル	24
各章ダイジェスト	25
サイバーセキュリティ対策9か条	26

## 第1章 まずはサイバーセキュリティの基礎を固めよう 27

1 最低限実施すべきサイバーセキュリティ対策を理解しよう	28
2 ①OSやソフトウェアは常に最新の状態にしておこう	30
2.1 パソコン本体とセキュリティの状態を最新に保とう	30
2.2 スマホやネットワーク機器も最新に保とう	31
3 ②パスワードは長く複雑にして、他と使い回さないようにしよう	32
3.1 パスワードの安全性を高める	32
3.2 機器やサービス間でのパスワード使い回しは「絶対に」しない	32
3.3 パスワードを適切に保管する	33
4 ③多要素認証を利用しよう	34
4.1 可能な限り多要素や生体認証を使い、秘密の質問にはまじめに答えない	34
4.2 パスワードはどうやって漏れるの？どう使われるの？	35
5 ④偽メールや偽サイトに騙されないように用心しよう	36
5.1 多様化する偽メールに注意しよう	36
5.2 公式サイト以外からアプリをインストールすることは控えよう	37
6 ⑤メールの添付ファイルや本文中のリンクに注意しよう	39
7 ⑥スマホやPCの画面ロックを利用しよう	40
7.1 スマホやパソコンには必ず画面ロックをかけよう	40
7.2 よくある情報の漏れ方と対策	41
8 ⑦大切な情報は失う前にバックアップ(複製)しよう	42
8.1 何をするにもバックアップを取ろう	42
8.2 ランサムウェアや天災にも対応できるバックアップ体制	43
9 ⑧外出先では紛失・盗難・覗き見に注意しよう	44
10 ⑨困ったときは1人で悩まず、まず相談しよう	45
コラム.1 攻撃されにくくするには、手間(コスト)がかかるようにする	46
コラム.2 利益が目的ではない攻撃に備えるには	47
コラム.3 セキュリティソフトを導入しても過信しないことが重要	48

## 第2章 よくあるサイバー攻撃の手口やリスクを知ろう

49

- 1 攻撃者に乗っ取られると起こることを知ろう ..... 50
  - 1.1 被害に遭わないために。そして加害者の立場にならないために ..... 50
  - 1.2 盗まれた情報は犯罪に使われる ..... 51
  - 1.3 乗っ取られた機器はサイバー攻撃に使われる ..... 52
  - 1.4 IoT機器も乗っ取られる。知らずにマルウェアの拡散も ..... 53
- 2 大きな脅威となっているランサムウェアを知ろう ..... 54
- 3 フェイクニュース、サイバープロパガンダに騙されないようにしよう ..... 55
  - コラム.1 最新の状態に保っても間に合わないゼロデイ攻撃 ..... 56

## 第3章 SNS・ネットとの付き合い方や情報モラルの重要性を知ろう

57

- 1 SNSなどのネットとの付き合い方、守り方を知ろう ..... 58
  - 1.1 SNSなどのネットの楽しみ方と気を付けること ..... 58
  - 1.2 SNSやネットの怖さ、こんなことが実際に起こっている ..... 59
  - 1.3 SNSやネットとの付き合い方の基本 ..... 60
  - 1.4 ネットいじめに気を付けよう ..... 61
  - 1.5 モラルを逸脱すると炎上を生む ..... 62
  - 1.6 望まない情報流出、流出したら消すことは難しい ..... 63
  - 1.7 こどもにスマホを持たせるとき「スマホ契約書」の提案 ..... 64
  - コラム.1 GPS、位置情報、ジオタグの管理 ..... 66
  - コラム.2 屋外でのゲームを安全に楽しむ。ながらスマホは×！ ..... 67
- 2 インターネットで守るべき法律やマナーを知ろう ..... 68
  - 2.1 アニメ・マンガ・音楽の違法な共有。パクリなどの著作権侵害 ..... 68
  - 2.2 ゲームの不正行為はNG／親しくてもプライバシーは守る ..... 69
  - 2.3 クラッキングはクールじゃない！ ..... 70
  - コラム.3 デマに踊らされない！ ..... 71
  - コラム.4 法律に違反することをしてはいけません。気軽に考えてはダメ ..... 72
  - コラム.5 成人年齢18歳引き下げに伴って注意が必要なこと ..... 73
- 3 便利なサービスや機能を利用して家族を守ろう ..... 74
  - 3.1 こどもを守る ..... 74
  - 3.2 お年寄りを守る ..... 76
  - コラム.6 デジタル遺産相続 ..... 78

## 第4章 災害・テロ、海外でのトラブル、普段とは違う環境のリスクに備えよう

79

- 1 大災害やテロに備えよう ..... 80
  - 1.1 まずは自分の身の安全を確保する ..... 80
  - 1.2 電池をもたす、情報収集をする ..... 81
  - 1.3 ラジオ、車載テレビを使った情報収集 ..... 82
  - 1.4 徒歩帰宅、海外での災害やテロに備えて ..... 83
  - コラム.1 国により異なる情報の取扱。海外でトラブルに巻き込まれないように ..... 84
- 2 屋外・海外でのインターネットの利用には注意しよう ..... 86
  - 2.1 一見なものにもないように見えて、危険がいっぱい ..... 86
  - 2.2 インターネットカフェの利用 ..... 87
  - 2.3 海外でスマホやタブレットを活用するために ..... 88
  - コラム.2 災害時の情報収集について ..... 90

## 第5章 スマホやパソコン、IoT機器を安全に利用するための設定を知ろう

91

- 1 スマホのセキュリティ設定を知ろう ..... 92
  - 1.1 スマホにはロックをかけ、席に置いて離れたり、人に貸したりするのは× ..... 92
  - 1.2 不安な人は携帯キャリアのセキュリティ対策プランを検討しよう ..... 93
  - 1.3 総務省によるシニア向けスマホ活用支援事業を活用しよう ..... 93
  - 1.4 情報漏えいを防ぐ ..... 94
  - 1.5 スムーズな機種変更と、予期せぬデータ流出の防ぎ方 ..... 96
- 2 パソコンのセキュリティ設定を知ろう ..... 98
  - 2.1 パソコンを買ったら初期設定などを確実に ..... 98

2.2	暗号化機能などでセキュリティレベルを高める	99
2.3	マルウェア感染に備え、3-2-1のバックアップ体制を整える	100
2.4	売却や廃棄するときはデータを消去する	101
2.5	紛失・盗難のとき、スマホとパソコン、どちらが安全？	102
コラム1	ダブルラインでトラブルに備える	103
3	IoT機器のセキュリティ設定を知ろう	104
3.1	常にインターネットに接続するIoT機器は注意が必要	104
3.2	購入後は初期パスワード変更などの設定を	105
4	それでも攻撃を受けてしまったときの兆候と対処を知ろう	106
コラム2	軍事スパイ、産業スパイに狙われてしまったら	108

## 第6章 パスワードの大切さを知り、通信の安全性を支える暗号化について学ぼう 109

1	パスワードを守ろう、パスワードで守ろう	110
1.1	パスワードってなに？	110
1.2	3種類の「パスワード」を理解する	110
1.3	「PINコード」と「ログインパスワード」に求められる複雑さの違い	110
1.4	「暗号キー」に求められる複雑さ	112
1.5	総当たり攻撃以外のパスワードを破る攻撃や生体認証を使った防御	112
1.6	多要素認証を活用する。ただしSMS認証は避ける	113
1.7	二段階認証と二要素認証と多要素認証の安全性	114
1.8	パスワードの定期変更は基本は必要なし。ただし流出時は速やかに変更する	114
1.9	パスワード流出時の便乗攻撃に注意	115
1.10	適切なパスワードの保管	115
1.11	パスワード情報をクラウドで保管する善し悪し	116
1.12	ノートやスマホを失くした場合のリカバリ考察	116
1.13	注意すべきソーシャルログイン	117
1.14	権限を与えるサービス連携にも注意	118
コラム1	暗号化の超簡単説明	118
コラム2	パスワードの管理と流出チェックについて	120
コラム3	パスワードを記録する演習	122
2	安全な無線LANの利用を支える暗号化について学ぼう	124
2.1	それぞれの状況に合わせた暗号化の必要性	124
2.2	無線LAN通信(Wi-Fi)の構成要素	124
2.3	暗号化無しや、方式が安全ではないものは危険	126
2.4	暗号化方式が安全でも「暗号キー」が漏れれば危険	126
2.5	会社などでの安全な無線LANの設定(暗号化方式)	126
2.6	会社などでの安全な無線LANの設定(その他)	127
2.7	公衆無線LAN利用時の注意	128
2.8	個別の「暗号キー」を用いる方式の公衆無線LAN	128
2.9	公衆無線LANに関して新規に購入したスマホなどで行うこと	129
2.10	公衆無線LANが安全ではない場合の利用方法	130
2.11	自前の暗号化による盗聴対策	130
2.12	まとめて暗号化するVPN	130
3	安全なウェブサイトの利用を支える暗号化について学ぼう	132
3.1	無線LANの暗号化とVPNの守備範囲	132
3.2	すべての通信と、その一部であるウェブサイトとの通信	132
3.3	httpsで始まる暗号化通信にはどんなものがあるか	132
3.4	より厳格な審査の「EV-SSL証明書」	134
3.5	アドレスバー警告表示と、常時SSL化の流れ	134
3.6	有効期限が切れた証明書は拒否する	134
3.7	他にも証明書に関する警告が出るウェブサイトは接続しない	134
3.8	ウェブサービスのログインは多要素認証を選択する	135
3.9	多要素認証すら破る「中間者攻撃」	136
3.10	ウェブサイトを使ったサイバー攻撃に対応する	136
4	安全なメールの利用を支える暗号化について学ぼう	138
4.1	メールにおける暗号化	138
4.2	送信の暗号化と受信の暗号化	138
4.3	メールにおける暗号化の守備範囲	138
4.4	メール本文の暗号化	139

4.5	怪しいメールとはなにか	140
4.6	マルウェア入りの添付ファイルに気を付ける	140
4.7	ウェブサービスなどからのメールアドレスの流出	142
4.8	流出・スパム対策としての、変更可能メールアドレスの利用	142
4.9	通信の安全と永続性を考えた SNS やメールの利用	142
5	安全なデータファイルの利用を支える暗号化について学ぼう	144
コラム4	「無料」ということの対価はなにか	146
コラム5	クラウドストレージサービスからの情報流出。原因は？	148

## 第7章 中小組織向け セキュリティ向上が利潤追求につながることを理解しよう 149

1	社内・社外のセキュリティを向上しよう	150
1.1	セキュリティ対策を実施して負のコストを発生させない	150
1.2	セキュリティ対策に必要な投資資金を確保する	151
2	災害時の会社のために事業継続計画 (BCP) を作ろう	152
2.1	打たれ強くあるために、どこでも作業できる能力	152
2.2	人的損失をリカバリする能力	153
3	テレワークとアウトソーシングをうまく利用しよう	154
3.1	テレワークと BYOD-Bring Your Own Device	154
3.2	効率的なアウトソーシング	155
4	ファイルの共有設定や情報の公開範囲を見直そう	156
5	企業が気を付けたいサイバー攻撃を知り、情報収集に心掛けよう	158
5.1	脅威や攻撃の手口を知ろう	158
5.2	より能動的に情報収集しよう	159
6	企業が気を付けたい乗っ取りのリスクを理解しよう	160
6.1	サプライチェーン攻撃やオフショア開発によるリスク	160
6.2	問題が起きると事業継続に影響を及ぼす	161
7	企業が気を付けたいサイバー攻撃の具体例を知ろう	162
7.1	標的型メール攻撃の具体例	162
7.2	フィッシング攻撃の傾向	163
7.3	不正アクセスの傾向	164
7.4	不正送金の傾向	165
7.5	ランサムウェアの傾向	166
7.6	ウェブサービスへの不正ログイン	166
7.7	ウェブサイトの改ざんや SNS の乗っ取り	167
7.8	DDoS 攻撃	167
7.9	サイバーセキュリティ以前の情報モラル教育を怠らない	168
8	個人情報情報は法律に則り適切に取り扱おう	169
9	フリー素材の取扱と著作権について注意しよう	170
10	取引先の監督を徹底しよう	172

## 付録 知っておくと役立つサイバーセキュリティに関する手引き・ガイダンス 173

付録01	セキュリティ担当者は知っておきたい「サイバーセキュリティ関係法令 Q&A ハンドブック」とは	中小組織向け	174
付録02	サイバー攻撃を受けた場合①～情報関係機関への相談や届け出	一般国民向け 中小組織向け	175
付録03	サイバー攻撃を受けた場合②～警察機関への相談や届け出、ガイドライン	中小組織向け	176
付録04	IPA が取り組むさまざまな中小企業向けセキュリティ対策支援	中小組織向け	177
付録05	IPA のより深いセキュリティ設定資料	中小組織向け	181
付録06	セキュリティ系業務のアウトソース	中小組織向け	181
付録07	中小企業がもっとクラウドサービスを利用しやすく！～認定情報処理支援機関 (スマート SME サポーター)	中小組織向け	182
付録08	セキュリティの資格取得を目指そう	一般国民向け 中小組織向け	183
付録09	セキュリティスキルを向上させるには「CYDER」と「CTF」	中小組織向け	184
付録10	本格的な普及がはじまったマイナンバーカード～よくある誤解やセキュリティについて	一般国民向け 中小組織向け	185

おわりに～インターネットとよい付き合いを続けるために	189
用語集	190
NISC 関連ウェブサイト、SNS 一覧	205
索引	206



## はじめに

みなさん、はじめまして。私たちは内閣サイバーセキュリティセンター(NISC)です。日本の政府機関で、国のサイバーセキュリティ政策を担当しています。突然ですが、世界中のコミュニケーションの手段と聞いたら、みなさんは何を思い浮かべるでしょうか？手紙、会話、写真、プレゼント、などいろいろなものを連想されるかもしれません。

その中でも、形は見えないけれど現代においては「インターネット」という技術が主役の1つだろう、と何となく意識されている方も多いのではないのでしょうか。

インターネットによりコミュニケーションのスタイルは大きく変わりました。インターネットが普及していない昔は、どんな場所にも設置されていた公衆電話で連絡を取るのは普通でしたが、インターネットが身近になると小型化された携帯電話、いわゆるガラケーが普及しまし

た。当時のインターネットの通信速度では、ガラケーを使って短い文章、すなわちメッセージを送る形のコミュニケーションが主流でした。

そして現代、インターネットの通信速度も安定し、大半の国民がパソコンだけでなく、スマホを所有しています。スマホは単なる電話機ではなく、「持ち歩ける小さなパソコン」と呼べるほど多機能なもので、基本的には常にインターネットに接続しています。多くの人がスマホやパソコンからチャットしたり、SNSで写真を送りあったり、映像付きのインターネット電話を使ったりして、家族や友人とのコミュニケーションを楽しんでいます。コミュニケーションの用途以外にも、調べたいことがあればブラウザでウェブサイトを検索したり、オンラインストアで買い物をしたりして、インターネットにつながったサービスに多くの人が慣れ親しんでいます。またクラウドと

呼ばれるインターネット上のサーバから業務上必要なデータの保存・共有をしたり、コロナ禍で普及したテレビ会議アプリでリモート会議をしたりと、仕事で多用している人もいでしょう。さらには社会保障や税関係など、スマホやパソコンがあればできる行政機関への申請・申告も増えています。

もはや現代において、スマホやパソコンからインターネットにつながり、民間企業・公的機関問わず、無料・有料含めて、さまざまなサービスを利用することは、家庭や職場、学校と生活のあらゆる場面で求められています。多様なサービスにつながり多くのコミュニティが形づくられ、インターネット上には1つの社会領域といえる「サイバー空間」が形成されています。

そのような便利で欠かすことのできないサイバー空間は、地域や老若



男女問わず、全国民が参画する基礎的なインフラであると呼べ、私たちが社会経済活動を営む上で重要かつ公共性の高い場として位置付けられるものです。

しかし、このサイバー空間、便利さもあれば、問題もあります。

世界中の人と距離を超えてつながるため、中には、自らの利益や自己顕示のために平気で他人の情報や財産を奪おうと悪事を働く者ともつながってしまいます。そのような悪事を働く者は、ありとあらゆる手段を用いて、スマホやパソコン、ルータなどのIT機器に対して、「マルウェア」という不正なプログラムを送りつけようとしています。インターネットにつながるということは、常にそのようなサイバー攻撃のリスクにさらされているのです。

また、SNSなどで自分の発言を広く読んでもらい自由に他の人と交流できることは、インターネットにつ

ながることで享受できるメリットの1つですが、接する人が常に自分と友好的な意見であるとは限りません。感情的になり、誹謗中傷といえるような発言が飛び交うことも珍しくありません。しかし、SNSでの発言から、精神的に追い詰められ、自らを傷付ける行為を選んでしまう人や事例も残念ながら生じています。面と向かって言えないような他人を傷付ける発言は、インターネット上でも決して発信してはいけません。

サイバー空間が、人々のくらしと密接につながり基礎的なインフラとなりつつある中、国民全員が、誰一人取り残されずその恩恵を享受していくためには、国民一人ひとりが能動的にサイバー空間における攻撃や脅威の存在を知り、サイバーセキュリティに関する素養・基本的な知識を身に付けていくことが必須です。スマホやパソコンを使ってインターネットにつながるときは、みんなが

常にサイバーセキュリティ対策を心掛けるべきなのです。

そのため本書では、サイバー攻撃の手口やリスク、そして被害とはどんなものがあるのかをイメージしやすくするために、身近な具体例を取り上げながら解説しています。そして、被害を受けないようにするにはどんな対策をすればよいのか？また被害を受けてしまった場合はどんな対処をすればよいのか？についても、具体的な手順や頼れる相談窓口を紹介しています。

ほかにも、

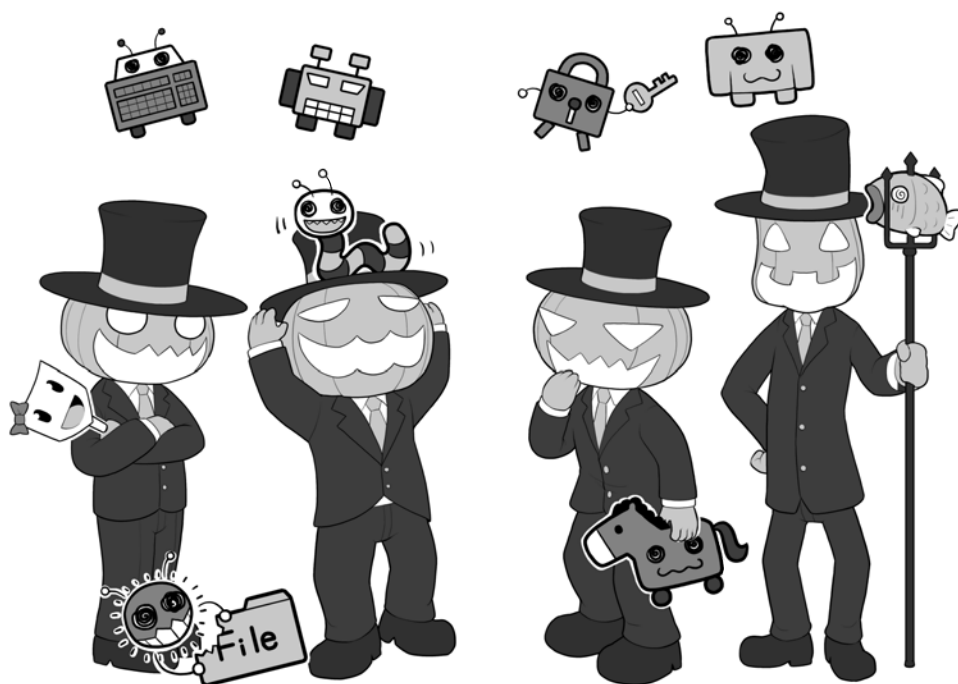
- ・サイバー攻撃を防ぐための基本となるパスワードの適切な管理
- ・こどもやシニアが安全にインターネット上のサービスを利用するための方法
- ・SNSなどで多くの人と交流する際に気を付けたいマナーや法律
- ・スマホやパソコンを不安なく利用するための設定

このイラストはインターネット上の悪意の人たちである攻撃者と、彼らが使う武器である「コンピュータウイルス（正確にはマルウェア）」をキャラクターにしたものです。

サイバー空間（インターネット）を悪意を持って利用し、自らの利益のためには他人の情報や財産を容赦なく奪い、ときにサイバー攻撃を通じて自己顕示欲を満たすといった、さまざまな悪事を働きます。

また、彼らが普通の人の仮面を被り、あるいは普通の人々が彼らの仮面を被ることもあります。

解説のイラストではそのあたりをきちんと描き分けていきますので、じっくり見てくださいね。



・災害や海外など普段とは違う環境でインターネットにつながる  
ときの事前の対策

・インターネットにおける通信の  
安全性を支える暗号化の基本

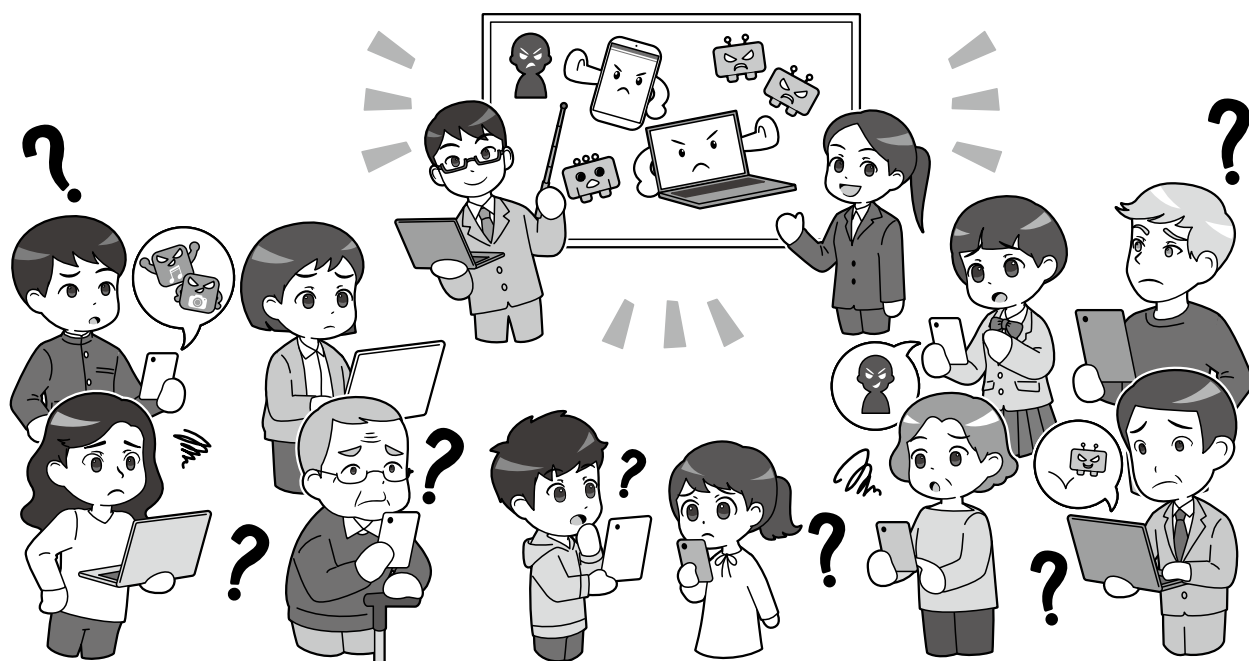
・中小組織のセキュリティ部門担  
当者に役立つ情報

など、サイバーセキュリティ対策に必要な内容を幅広く取り上げ、いずれも読む前には専門知識を必要とし

ない形でやさしく説明しています。  
本書を読んで、安全・安心なサイバー空間を一緒に作っていきましょう。

また、NISCでは、本書だけでなく、  
「みんなで使おうサイバーセキュリティ・ポータルサイト」を運営して、サイバーセキュリティの普及啓発や人材育成に取り組んでいます。

ポータルサイトでは、こども、シニア、企業の一般社員・経営者など対象者別に適したセキュリティ施策の紹介や、セキュリティ施策におけるセミナーやイベントの実施状況などを公開しています。本書やポータルサイトをご覧ください、国民一人ひとりのサイバーセキュリティ対策の意識を高められれば幸いです。



## 「みんなで使おうサイバーセキュリティ・ポータルサイト」

<https://security-portal.nisc.go.jp/>

### ※ご注意

本書では、初心者の方にサイバーセキュリティ関連の問題を理解してもらうために、実際のケースと比較してわかりやすく簡略化したり、内容を理解しやすいように関連する事項の一部を省略したりして記述している場合があります。ご了承ください。

このハンドブックを読んで、よりサイバーセキュリティに関する理解を深めていきたいと思う方は、ぜひステップアップして、さまざまな専門誌や最新の記事にチャレンジしていただくと幸いです。

なお、登場する人物、および、団体は架空のものであり、実在するいかなる人物・団体とも関係はありません。



## プロローグ

# インターネットにある基本的なリスクや トラブルを知ろう

私たちは、スマホやパソコンを用いて、いつでもどこでもインターネットにつながり、便利なサービスを利用したり、世界中の人とコミュニケーションしたりできます。しかしインターネットには、注意したいリスクやトラブルがあります。まずは本書全体を通じて登場する基本的なリスクやトラブルについて知しましょう。

## 1 サイバー攻撃とは？

---

## 2 ハッカーと攻撃者とは？

---

## 3 攻撃者が使う武器「マルウェア」とは？

---

3.1 どんな種類があるの？

3.2 どのような機能を持つものがあるの？

3.3 どんなものが感染したり、感染させたり、悪さをするようになるの？

## 4 サイバー攻撃の具体例は？

---

4.1 どんな攻撃があるのか？

4.2 会社や団体が狙われるとどうなる？

## 5 攻撃者とはどんな人物なの？

---

## 6 どうやって攻撃されるの？

---

6.1 主にマルウェアなどを使って「技術的」に攻撃

6.2 人の心の隙を突く心理的な攻撃～ソーシャルエンジニアリング

## 7 SNSやネットのコミュニケーションで注意したいことは？

---

7.1 SNSやネット上の誹謗中傷対策

7.2 SNSやネット上の犯罪やトラブル

# 1

## サイバー攻撃とは？

### よく聞く「サイバー攻撃」とは？



サイバー攻撃は、誰がなんの目的でやっているのでしょうか。

軍事スパイや産業スパイ？ それともハッカー？

いわゆるスパイ▶用語集 P.197 の目的は、軍事機密や先進の研究内容など、自国や企業にとって有益な情報の入手です。それに対し、私たちが普段遭遇するサイバー攻撃は、主として個人情報や金銭など、攻撃する者にとって利益が得られることにつながることを目的としています。

スパイは、目標の達成が絶対条件であり、ありとあらゆる手段で攻撃を行うため、どんなにセキュリティ

が厳重でも侵入してきます。それは、やっかいな存在で、現状完璧には防ぐことができません。

一方、利益目的のサイバー攻撃は、攻撃する者にとってはビジネスとしての性格を帯びています。例えば、「ここはセキュリティがしっかりしているので手間がかかる(≒費用がかかる)のでやめよう」「ここなら手間がかからない(≒安くすむ)からここから盗もう」というように、攻撃しやすい方に流れる傾向があり、セキュリティレベルを高めることで、ある程度攻撃を受けにくくすることができます。完璧に防ぐことは

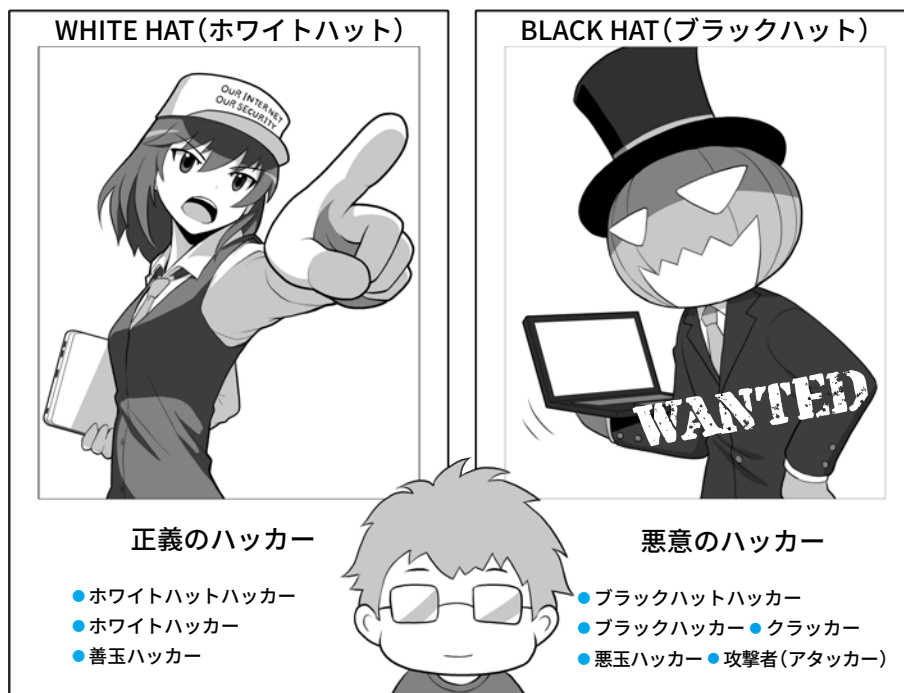
難しくても、努力をすれば被害に遭う確率を減らせると考えてよいでしょう。

サイバー攻撃への対処は、ヒーローが登場する勧善懲悪のアニメのように、きっちり解決をしたり、あるいは0と1のデジタルのようにかっちり防いだりすることはできません。まずは安全を確保する手段を、石垣を築くように地道に積み上げる必要があるのです。

これから、私たちが説明していくサイバーセキュリティに関するお話は、この考え方に沿っていることを覚えておいてください。

# ハッカーと攻撃者とは？

## 「ハッカー」の意味やさまざまな呼称



そもそも「ハッカー」とはコンピュータの知識と技術に精通した人を尊敬して呼ぶ名前で、イコール悪事を働く人という意味ではありません。その用語を自分で使うとき、あるいは報道など見るとき、どのような意味で使われているのかを気かけましょう。

サイバーセキュリティが専門でない新聞や雑誌、テレビでは、サイバー攻撃を行う悪意の人たちを「ハッカー」▶用語集 P.201 と呼びがちです。しかし、この呼び方はやや正確ではありません。

ハッカーとは、もともとはコンピュータに精通し、その方面の高い知識と技術を持つ人を指すある種の尊称であり、イコール悪事を行う攻撃者▶用語集 P.196 ではありません。

そして彼等がその技術を駆使して行う作業を「ハッキング」や単に「ハック」といいますが、これも本来は悪事と直接結びつくものではありません。

ん。

ただしこういった知識や技術をもって悪事を行う人も存在するため、それらを善意の人と区別する意味で、「ブラックハットハッカー」や「ブラックハッカー」、あるいは防御しているものを割って侵入することを意味する「クラッキング」▶用語集 P.196 から転じて「クラッカー (cracker)」▶用語集 P.195 や攻撃者の意味を持つ「アタッカー (attacker)」▶用語集 P.194 と呼ぶのです。

一方、日本語で「ハッカー」と安易に呼ばない場合は「悪玉ハッカー」や「悪意のハッカー」▶用語集 P.193 ともし

われます。(本書ではこれらの人を「攻撃者」「悪意のハッカー」などと呼びます)

逆に善意に基づいて高い知識や技術を使う人を「ホワイトハットハッカー」や「ホワイトハット」「ホワイトハッカー」といい、日本語では「善玉ハッカー」や「正義のハッカー」と呼びます。

本書では、この本来の意味に基づいた用語で解説しますので、みなさんにもぜひ覚えてもらって、日常生活でも正しい名称が広く用いられるように協力してくださいね。

# 3

## 攻撃者が使う武器 「マルウェア」とは？

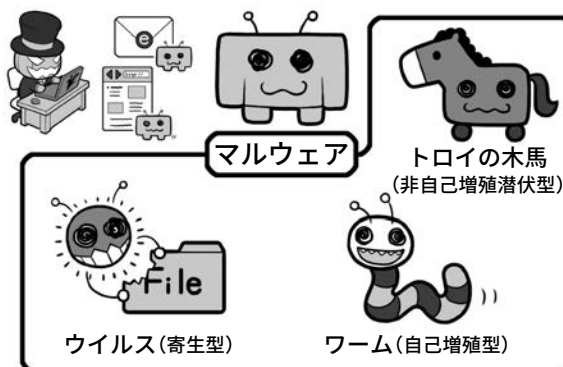
### 3.1 どんな種類があるの？

先ほどのハッカーの例と同じように、今1つ正しく用いられていないのが、「コンピュータウイルス」や、単に「ウイルス」という用語です。

攻撃者がサイバー攻撃を行う場合、相手のコンピュータをなんらかの悪意のプログラムに感染させ、これをコントロールする方法がよく用いられます。この攻撃に使われるプログラムをまとめて「ウイルス」と呼びがちです。しかし、悪意のプログラムは本来「マルウェア」▶用語集 P.203 もしくは「不正なプログラム」と呼ぶのが正しく、「ウイルス」とはその中の一種で、コンピュータ上のファイルが感染し、そのファイルに寄生して活動するタイプのものを指す限定的な名称なのです。現実世界に例えるなら「マルウェア」とは病気を起こす原因の総称「病原体」にあたり、「病原体」の一種で細胞に寄生しないと増殖できないものを「ウイルス」と呼ぶのと同様です。そして病原体にはウイルスの他にも、単独で存在することができる細菌、原虫や寄生虫などがあります。マルウェアにも同様に、独立していて非自己増殖型の「トロイの木馬」と呼ばれるものや、独立していてかつ自己増殖型の「ワーム」があります。

また、機能による分類としては「ボット」▶用語集 P.203「ランサムウェア」▶用語集 P.203「キーロガー」などの呼び方もあります。これは病原体の行動形態を表す病気の症状の名前のよう

### マルウェアにはどんな種類があるの？



### どんな機能を持つの？



なものです。ただ、一般に広がった「ウイルスという言葉がマルウェアと同じ意味で使われる」事実もあるため、その整合性を取るために「広義のウイルス」といったいい方も存在します。みなさんには、このことも覚えていただいて、正しい呼び方を広めてもらうと同時に、新聞、雑誌やテレビで「ウイルス」と使われているときは、それが「広義のウイルス＝マルウェア」の意味なのか「狭義のウイルス＝ファイルに寄生する感染プログラム」なのかを文脈から読み取って、正しく理解してもらえとうれしく思います。

### 3.2 どのような機能を持つものがあるの？

マルウェアの主な機能をあげると

このようになります。

#### ・悪意のボット (Bot)

ボットとはRobotの略で、悪意のものは感染するとコンピュータが攻撃者に乗っ取られ、別のコンピュータへの攻撃などに使われる

#### ・ランサムウェア

感染すると、コンピュータ上のファイルが暗号化▶用語集 P.194 された上で、攻撃者から元に戻すための身代金を要求される

#### ・キーロガー

比較的古いマルウェアで、感染するとキーボードの入力を記録して攻撃者に送信する。攻撃者はこれを利用してパスワード▶用語集 P.200などを盗む

また、例えば「トロイの木馬」は、最初にコンピュータに侵入するときには害がないようなふりをして、侵入

したらマルウェアの本性を現したり、外部からボットやランサムウェアを呼びこんだりして悪事を働き始めます。

### 3.3 どんなものが感染したり、感染させたり、悪さをするようになるの？

マルウェアに感染するものといえば、おそらく真っ先にパーソナルコンピュータ(以下パソコン)やスマートフォン(以下スマホ)、タブレットなどを想像するでしょう。

「マルウェアはコンピュータが感染する悪意のプログラム」

この表現も間違いではありません。しかし、実際には、会社などで使っている無線LAN(Wi-Fi)アクセスルータ▶用語集P.203、ネットワークプリンタ、監視カメラ、スマートテレビ、ネット接続医療機器、変わったところではPOSレジ▶用語集P.191、なども感染するそうです。コンピュータではないのになぜ感染するのでしょうか。

この「コンピュータが感染する」と「そう見えないものまで感染している」ことの矛盾を解く鍵は、「現代の電子機器は、コンピュータに見えないものでも、コンピュータを内蔵している」ところにあります。

こういった機器がインターネットにつながりデータをやりとりする以上、マルウェアに感染する可能性があるわけです。

とくにIoT(Internet of Things)▶用語集P.191、「モノのインターネット」の時代が訪れ、私たちの周りに存在するありとあらゆる機器がコンピュータ化し、インターネットにつながると、今より多数の機器が感染する可能性があります。

ただし、こういったマルウェアに感染してしまうかもしれないことや

### どんなものが感染したり、感染させたり、悪さするようになるのか



りも、もっと深刻な問題があります。それは人間の心の隙を突いたサイバー攻撃です。

機器を強制的にマルウェアに感染させるためには、セキュリティホール(脆弱性)▶用語集P.198と呼ばれるプログラム上の弱点が必要です。セキュリティホールがあるということは、家の鍵が壊れているようなものです。しかし、日々セキュリティのアップデート▶用語集P.194＝修正対応が行われ、たいていのセキュリティホールはすぐにふさがれます。

そういった場合でも、所有者をだまして自らインストール▶用語集P.194させれば、外から無理矢理侵入せずとも、簡単に悪事を働くことが可能のようにしてしまえるのです。

これを実現するのが後ほど説明する「標的型メール」▶用語集P.201など、人間の心の隙を突くタイプの攻撃です。問題はこの心の隙が、コンピュー

タのセキュリティホールのように簡単には塞げないことにあります。セキュリティ意識は、本人が必要性を認識しないと向上しないからです。

サイバー攻撃に対するIT機器の防御をいくら固めても、人間をだます攻撃手法はいくつも存在し、こちらはなかなか防げない。このこともよく知ってください。

そして被害者が友人や職場の仲間にならに感染を広げていって、さまざまな機器が持ち主の知らぬところで乗っ取られ、攻撃者によるサイバー攻撃に勝手に使われることもあるのです。

そう、被害者であるはずのあなたが、いつの間にか攻撃に参加させられ、ときに加害者の立場に立たされることもありうるのです。

まずは防ぐための知識を得て行動をおこしましょう。



# 4

## サイバー攻撃の具体例は？

### 4.1 どんな攻撃があるのか？

サイバー攻撃というと、まるで小説や映画の世界の話かと思いませんか？実はあなたの会社や団体などの、すごく身近なところでも日常的に起こっていることなのです。

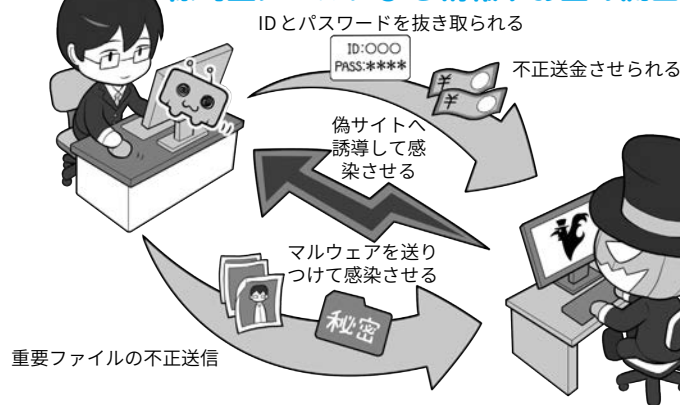
サイバー攻撃として代表的なものは、みなさんが普段業務に使っているパソコンやスマホなどが、マルウェア（他者を攻撃する不正なプログラム。一般的にはコンピュータウイルスとも呼ばれる）に感染し、インターネットを通じて機密情報やお金が、流出させられたり盗まれたりするものがあります。

パソコンなどの脆弱性（弱点。以下セキュリティホール）▶用語集 P.197 を突き、知らないうちに感染させるものもありますが、その機器の所有者をだまして悪意の罠に飛び込ませたりするものもあります。例えば、電子メールに悪意のホームページ▶用語集 P.202（以下ウェブサイト）へ誘導するリンク▶用語集 P.204 や、添付ファイルに偽装したマルウェアを含ませ開かせるわけです。

メールのリンクや添付ファイルを開いて確認するといった作業は、ビジネスパーソンであれば毎日やっていることであり、そんな行動が、攻撃の糸口につながっているのです。

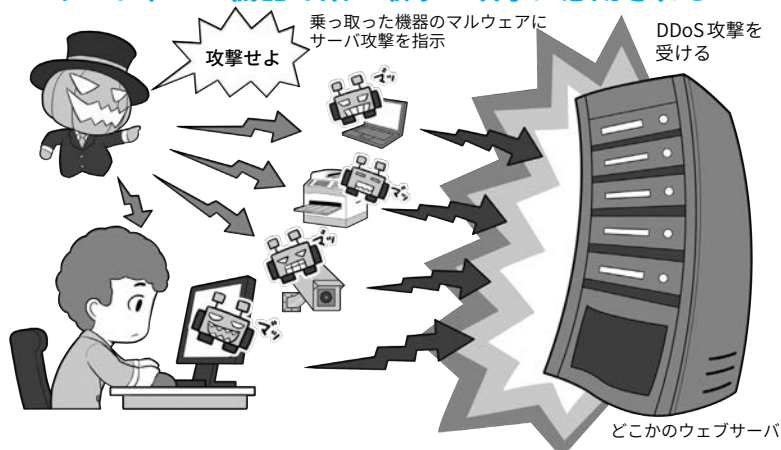
「マルウェアはとにかく、リンクで？」と思うかも知れませんが、リンク先を開いてみれば有名銀行のネットバンキングと瓜二つの偽サイトになっていて、ID▶用語集 P.191 とパ

#### 標的型メールによる情報やお金の流出



攻撃者はあなたから重要情報やお金を盗むために、マルウェアに感染させて重要ファイルを不正に送信させたり、偽のメールで偽の銀行サイトなどに誘導する「フィッシング詐欺」を行って不正送金させたりします。どういう方法でだまされてしまうのか、一度調べてみましょう。

#### パソコン、IoT機器の乗っ取り～攻撃に悪用される



所有するIT機器が悪意のボット用マルウェアに感染すると、攻撃者が管理する攻撃用の仕組みであるボットネットに接続され、あなたが知らないところでサイバー攻撃に参加させられることになります。気づかずに加害者の立場になってしまうかもしれません。

#### ランサムウェアに感染して業務停止



ランサムウェアに感染すると、パソコンなどのファイルを暗号化され、解除するためには身代金を要求されます。しかし、身代金を払っても解除するキーをもらえるとは限りません。普段からシステムやデータのバックアップを取って、元の状態に戻せるように備えましょう。どうやって侵入されるのか、実例の記事をさがして学んでみましょう。

スワードを入力させられ、それを使われ会社や団体の口座から不正送金されてしまい、被害に遭うケースも発生しています。

また、会社や団体のパソコンやIoT機器などがマルウェアに感染すると、情報流出だけでなく勝手に操作され、他の会社などへのサイバー攻撃に利用されることもあります。被害者のはずが突然加害者の立場になり、それらの事例が明らかになると社会的信用を失うかもしれません。

パソコンなどのデータを暗号化して読めないようにして、身代金を要求されるマルウェアも急増しています。身代金を払ってもデータが元どおりにならない場合もありますし、業務遂行ができなくなるので、なによりも事前の対策が大切です。

## 4.2 会社や団体が狙われるとどうなる？

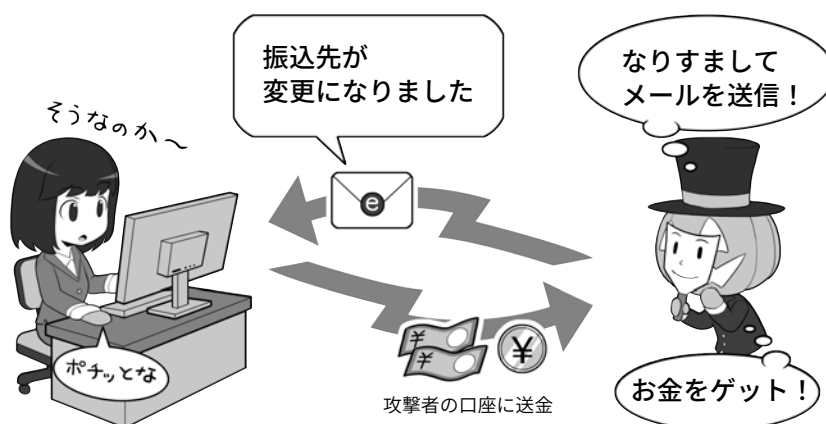
他にも電子メールが使われる事例としては「BEC(ビジネスメール詐欺)」▶用語集 P.190 があります。BECとは、攻撃する相手や環境を事前によく分析して行われる、企業などを対象としたビジネス用の詐欺メール攻撃です。

事前に支払い関係のメールを盗まれ分析され、取引先を装ったそっくりのメールが届けば、疑わずに振り込んでしまうことも十分に考えられることでしょう。

また、企業には株主に影響を及ぼす社外秘の情報というのは必ず存在しています。そういった情報を大企業から直接盗めなくても、セキュリティの甘い関連企業があれば、そこから盗んで売ればよいと考えるかもしれません。

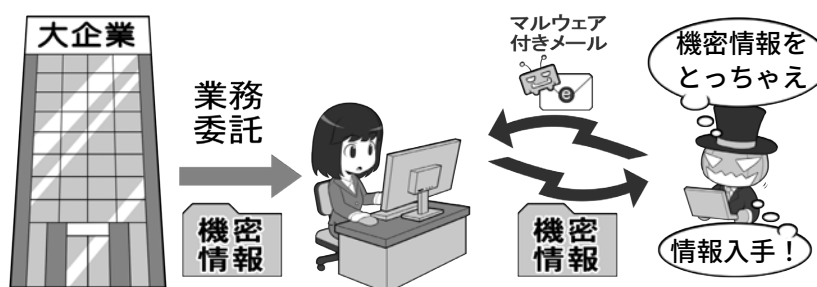
そうした特定の会社や団体を標的

### 取引先のふりをしてメールで送金請求



単純に「お金を送れ」といわれてもだまされる人はいませんが、取引先の企業の人になりすました攻撃者が、通常の請求書発行の業務として口座番号の変更を連絡してきたら、見分けることはできるでしょうか？ そういった攻撃を行うために、攻撃者は事前にメールサーバから業務メールを盗み、日常どういったやりとりをしているか、といったことまで下調べた上で攻撃してくることもあります。

### 取引先の情報流出で業務停止



攻撃者は情報を盗み出そうと思った場合、セキュリティの厳しい大企業よりも、セキュリティの甘い小さな会社を狙ったほうが簡単と考えます。外注を受けていればしめたものと考えます。

とした「サイバー攻撃」は、知らない間に所有するパソコンなどに入り込む不正アクセス、既に紹介したBEC、ランサムウェア他さまざまな手段で襲いかかってきます。

ちなみにBECは、国際比較したとき日本企業は被害報告が少ない傾向があります。日本企業では、多額の支払いには入念な確認を必要とするビジネスプロセスが構成されていることも被害が少ない要因の1つと考えられます。

ただしこれは、あくまで現時点の話であり、例えばビジネスプロセスが成熟していないスタートアップ企業などを狙ったBECが発生しないとも限らないため、注意を怠ってはいけません。

データが漏えいしたら発注元からは信用のならない取引先と判断されて取引が打ち切られることも十分に想定されます。とくに小さな会社やNPOなどにとってはまさに死活問題になり得るサイバー攻撃なのです。

# 5

## 攻撃者とはどんな人物なの？

### 攻撃者(アタッカー、クラッカー)とはどんな人物なのか

#### 悪意のハッカー



#### コスト優先

一口に攻撃者といってもそのカテゴリはいくつかに分かれます。

興味本位、自己顕示欲、腕試し、愉快犯などのアマチュア的な者、一般的な攻撃者（悪意のハッカー）ともいえる金銭目的でビジネスとして攻撃を行っている者、プロフェッショナルで産業的に目的の情報を狙う産業スパイ、そして国家のバックアップを受けなが

#### 産業スパイ



ら他国の軍事機密や、政治的な情報を盗み出したり、果ては SNS などを使って相手国に不利益を与えるプロパガンダなどの工作活動を行う国家的ハッカー（State sponsored hacker）などがいます。

これらは、必ずしも明確に分かれているわけではありません。国家、運営する主体、あるいはスポンサーによって、そのボーダーは

#### 国家的ハッカー



#### 目標達成優先

曖昧です。

ただ、一般的な悪意のハッカーはビジネスとしてハッキングを行うので、攻撃のコストに対して収入が見合わないほどセキュリティを固めれば避けられやすくなります。

一方、後者二つは「コストは考えず目標の達成が必須」なので、狙われた場合その攻撃を避けるのは困難です。

ここまでで、漠然と悪意を持った者＝攻撃者が存在することがイメージできたと思います。ではその悪意を持った人々は何者なのでしょう？

まず最もアマチュア的なものが、こどもの腕試しやスクリプトキディ  
▶用語集 P.197 と呼ばれる者です。こういった人物は「自分の力量を試す」「自己顕示欲を満たす」「興味本位」で攻撃を行います。ネットの見えにくいところでサイバー攻撃用のツールが販売されていることもあり、よく考えずにこれらを購入し、違法性を認識せず使う者もいるので侮れません。ただ単純に趣味や興味だけで攻撃を行う人は、最近のセキュリティ対策意識の高まりや法整備の状況が

ら、攻撃を仕掛けることによるリターンよりもリスクのほうが上回り、その結果相対的に少なくなっているように見えます。

次に金銭目的で行動する悪意のハッカーがいます。彼らはマルウェアを開発する能力や、身を隠す能力がありますが、活動は主に「金銭目的」のビジネスであり、仕事にコストパフォーマンス、つまり攻撃に手間をかけずに多く稼げることを望むので、防御のしようがあります。しかし金銭目的の攻撃者は多くの企業、個人に対して被害を及ぼしており、現在は組織化、相互連携を進める方向に進んでいます。単独で攻撃するよりは、チームを組んで得意な分野、技能を出し合い、利益の効率を上げ

ようとしているのです。

次に企業が持つ先進技術や製品計画などを盗もうとする産業スパイ、兵器開発や軍事計画の情報を狙ったり敵対国に誤情報の拡散で混乱を起こしたりしようとする軍事的ハッカーなどです。明確な目標を持つ攻撃者のため、狙われるとコストを度外視して何度も執拗に攻撃を仕掛けてきます。

このように攻撃者といっても様ではなく、愉快犯的な行動から、国の命運を左右する軍事目的まで多種多様なのです。しかし、いずれにしてもしっかりとしたセキュリティ対策が、防御を行うための入口なのはいうまでもありません。



## 6.1 おもにマルウェアなどを使って「技術的」に攻撃

では攻撃者は具体的にどう攻撃をしてくるのでしょうか。大きく分けると2つの方向性があります。1つは技術的な攻撃、もう1つは心理的な攻撃です。

マルウェアを使ってパソコンやスマホ、あるいはシステム上のセキュリティホールを突く、技術的で「サイバー攻撃」の要素が強いものが前者。「ソーシャルエンジニアリング」▶用語集 P.198 と呼ばれ、人間の心の隙を突く詐欺や「心理攻撃」の要素が強いものが後者です。本項では「サイバー攻撃」について解説します。

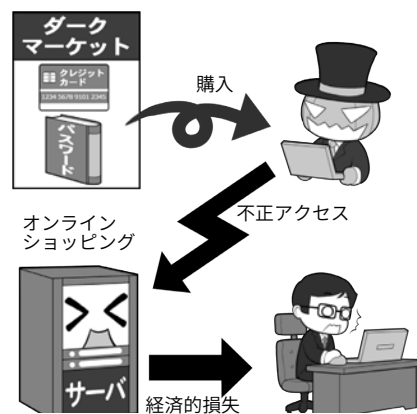
まずは、自分や自社が攻撃され自らが損害を受けるサイバー攻撃。代表的なのはマルウェアによる攻撃です。攻撃者はメールや偽サイトなどにマルウェアを仕込み、利用者が添付ファイルを開いたり、メールのリンクから不正なページを開いたりすると、会社のパソコンがこれに感染し、その結果社内システムに侵入されます。そうすると社内システム用のIDやパスワードが盗まれ、機密情報の流出が発生します。また、これらは乗っ取ったメールアカウントを使って、なりすましのメールが送る攻撃にもつながります。

次に自分や自社が気付かないうちに攻撃される例です。インターネットでは日々、さまざまなウェブサービスが攻撃されアカウント情報の漏えいが発生しています。例えば個人用のアカウントのIDとパスワード

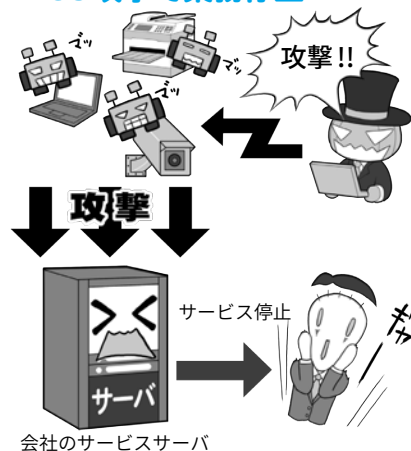
を会社用にも使い回ししていると、どこかのサービスから漏れた情報によって会社のシステムへの不正侵入や不正利用を許すことにつながります。また、業務でインターネット上のクラウドストレージサービスに重要情報を保存していると、ここから情報流出が発生するかもしれません。この例では「自分自身はマルウェアなどに感染した形跡がなくても攻撃される」ことを知って下さい。

最後に、自社が攻撃されるだけでなく他者にまで損害を与える例です。攻撃者が多数のIT機器にマルウェアを感染させた上で、それらのIT機器からターゲットにした他者のコンピュータなどに通常では考えられない量のデータをターゲットに送りつけ使えない状態にする「DDoS攻撃」▶用語集 P.190、パソコンの中身を勝手に暗号化して、暗号化の解除と引き換えに身代金を要求して脅迫する「ランサムウェア」などが挙げられます。自社で業務遂行をできなくなると、自らが被害に遭うだけでなく、関連する他社にも損失を与えます。また、業務が停止することで、業務に関連する顧客／サービス利用者にも間接的に経済的損失を与えます。

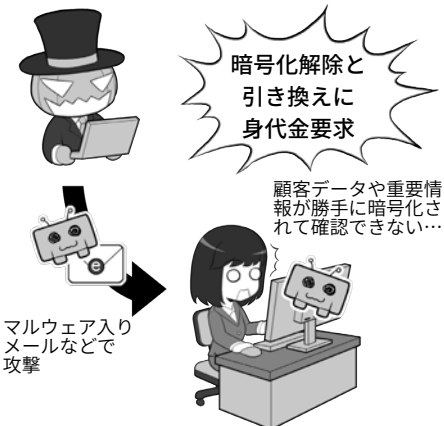
### 流出情報で乗っ取られて経済的損失



### ボットネットからのDDoS攻撃で業務停止



### ランサムウェアで暗号化して身代金要求



## 6.2 人の心の際を突く心理的な攻撃～ソーシャルエンジニアリング

さて「サイバー攻撃」ではない一般の犯罪で、みなさんがよく耳にするものはなんしょう。

たぶん「オレオレ詐欺」「振り込め詐欺」など、人をだましてお金を巻き上げる「特殊詐欺」でしょうか。関係機関が日夜注意喚起を行っていますが、未だに多くの方が被害に遭い続けています。

それが終わらない理由は、こういった特殊詐欺が人間が生まれながらにして持っている「心の際」というセキュリティホールを突いた「心理的攻撃」だからです。人間のセキュリティホールはなかなか埋められず、対策することが難しいからです。そしてサイバー攻撃でも、この人間の心の際を突いたものが多くあります。

例えば先ほど紹介した、BECの発端になったなりすましの詐欺メール。この攻撃の入口は、相手の心の際を突き、シンプルに「数行の文字で」だまされただけです。

また、送りつける相手をよく調査・分析した上で、送り付けられる偽装ファイルやリンクは、結果的にマルウェアを利用しますが、人間の心の際を突く手法です。

こういった心理的誘導による被害を軽減するためには、多くの人々がサイバーセキュリティ意識を向上させるだけでなく、人間の心の際をついた攻撃が存在することを認識し、予防する意識を持つことが重要です。

この狙った情報を、情報通信技術に限定せず心理的攻撃も組み合わせながら盗み出す攻撃を「ソーシャルエンジニアリング」と呼びます。



「ソーシャルエンジニアリング」は現実でもネットでも心の際を突いてだます

上はビジネス上のソーシャルエンジニアリング、下は振り込め詐欺の例ですが、こうやって見ると、実は2つの詐欺の本質的な部分は同じだと分かります。

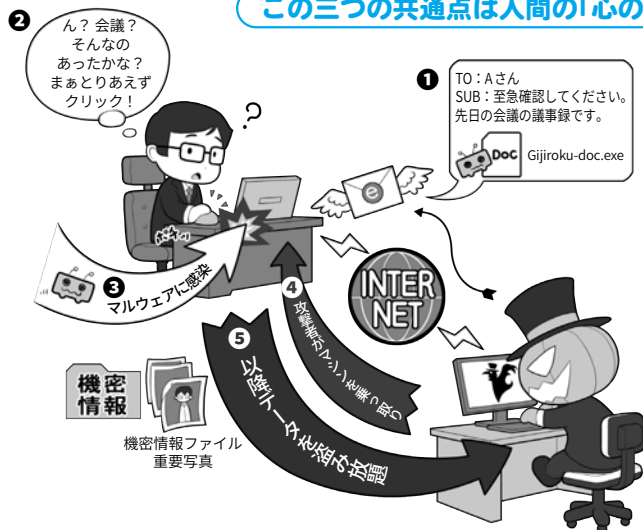
これらは上手く人間の心の際を作り出し、自らの望みどおりに相手を操る体系化されたテクニックなのです。振り込め詐欺の場合は、例えばまず相手に「身内が事故やトラブルを起こして大変だ!」と頭を混乱させ、相手が本来持っている冷静な判断能力を奪います。せかしたり、弁護士や警察官に扮した人物を登場させたり、お金を払えば助かると交換条件を出したりして、さらに追い込みます。



現実の世界

この三つの共通点は人間の「心の際」を突いた点

ネットの世界



こういった心理的な揺さぶりは、古典的なソーシャルエンジニアリング（≡心理的交渉テクニック）の、「ハリーアップ」▶用語集 P.201「ネームドロップ」▶用語集 P.200「ギブアンドテイク」▶用語集 P.195 などにあたるでしょう。

一方、ネットの世界のソーシャルエンジニアリングは、知り合いになりすまして「標的型メール」を送る場合、これらの「フレンドシップ」▶用語集 P.202 という手法の要素が使われています。ちなみに標的型攻撃メールにおいては、攻撃者が特定の組織へ攻撃を仕掛ける前に「トラッキング」▶用語集 P.200 と呼ばれるゴミ箱を漁る行為で、サーバーやルーターなどの設定情報、ID パスワードなどの情報を捨てられた資料から探ることがよくあります。

攻撃者は情報通信技術に限定せず心理的攻撃も組み合わせる攻撃を仕掛け、セキュリティを突破しようと試みます。

# SNSやネットのコミュニケーションで注意したいことは？

## 7.1 SNSやネット上の誹謗中傷対策

### SNSやネットで他人を傷つける発言をしてはいけません



SNS ▶用語集 P.192 は自由に自分の意見を発信できて便利ですが、議論が行き過ぎ感情的な発言をしてしまうことは誰にでもあります。SNS やネット上の過激な発言は、名誉毀損罪や侮辱罪などの犯罪となる場合もあります。対面でのコミュニケーションと同じように、他人を傷つけるような発言を SNS やネット上でも決して発信してはなりません。

総務省 HP | インターネット上の誹謗中傷への対策

[https://www.soumu.go.jp/main\\_sosiki/joho\\_tsusin/d\\_syohi/hiboutyusyou.html](https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/hiboutyusyou.html)

インターネット上の誹謗中傷への対応に関する政策パッケージの概要 (PDF)

[https://www.soumu.go.jp/main\\_content/000755959.pdf](https://www.soumu.go.jp/main_content/000755959.pdf)

サイバー攻撃のほかにも、私たちにとって身近な SNS やネットのコミュニケーションでは、気を付けたいトラブルがたくさんあります。とくに SNS は自分の発言を広く読んでもらい、自由に他の人と交流することができる便利なサービスですが、常に周りの人が自分と友好的な意見だとは限りません。議論が行き過ぎることもありますし、また、自分が気に入らない人に対しての表現がうっかり過激になってしまうこともあります。一方、誹謗中傷となるような批判的発言を多数人から受ける立場になってしまえば、精神的に極めて辛い立場に立たされることになり、残念ながら自らを傷つける行為を選ぶような人や事例も生じています。

SNS やネット上での誹謗中傷対策として、総務省では「インターネッ

ト上の誹謗中傷への対応に関する政策パッケージ」を発表しています。

その内容は、以下のとおりです。

- **ユーザーに対する情報モラル及びICTリテラシーの向上のための啓発活動**
- **プラットフォーム事業者の自主的取組の支援と透明性・アカウントビリティの向上**(SNS 事業者による削除等の自主的取組を支援すると共にその状況把握を行うものです。)
- **発信者情報開示に関する取組**(他者の権利を侵害する発言に対し削除や損害賠償などの権利行使を行う前提として、発信者を特定するための制度の整備です。)
- **相談対応の充実に向けた連携と体制整備**(誹謗中傷などの被害を受けた人が相談を行う窓口間の連携強化と相談員の増員など

を行うものです。)

また、ネット上の過激な発言は、名誉毀損罪や侮辱罪などの犯罪となる場合もあります。名誉毀損罪と侮辱罪の違いは、事実の指摘があるかどうかですが、SNS やネット上で対象を過激に傷つけるような「ゴ〇〇ズ」や「ま〇けやろう」などの発言は侮辱罪にあたる可能性があります。侮辱罪の法定刑が令和4年7月7日より引き上げられています。それまで侮辱罪の刑は、拘留または科料という極めて軽く、例外的な場合を除き、逮捕がされない内容でしたが、今では、1年以下の懲役若しくは禁錮若しくは30万円以下の曝気又は拘留若しくは科料とされ、逮捕の可能性もあるものとなっています。誹謗中傷的発言をしないように注意しましょう。



## 7.2 SNSやネット上の犯罪やトラブル

SNSやネットでコミュニケーションする際、注意すべき犯罪もたくさんあります。

例えば、「なりすましや誘拐・略取」。SNSなどで未成年と同じ年齢や性別になりすまして近づき、その上で相手を誘い出して誘拐や略取などに及ぶケース。あるいはSNSで家出などをしたこどもの書き込みを見付けて、自宅などに連れ込むケースもあります。

また、同じようにネットで未成年のふりをして近づき、相手の警戒心を和らげて、「私も送るからあなたも送って」と裸の写真を要求して、入手したらその写真を使って相手を脅迫するケースもあります。

このような、こどもたちが自分自身の裸の写真を撮り、交換し合うことによって起こる被害を「自画撮り（セクスティング）」被害といいます。一度自分のスマホなどに記録された写真は、流出の危険がありますし、相手に渡してしまえばネットに流され、その後ずっと自分を苦しめ続ける可能性があることを考えなくてはなりません。こどもに限らず、交際していた相手が別れたことの腹いせに、裸の画像をインターネットに流す犯罪「リベンジポルノ」としても問題になっています。

またSNSへの投稿やSNSのグループチャットで、誰かの悪口をいったりする「ネットいじめ」は、やっている本人たちは軽い気持ちでも、時に相手を激しく追い込んで悲劇を招いたりすることもあります。現実世界のいじめ同様、絶対にやってはいけないことです。

### なりすましや誘拐・略取(連れ去り)



#### 後日、会う約束をしたら…



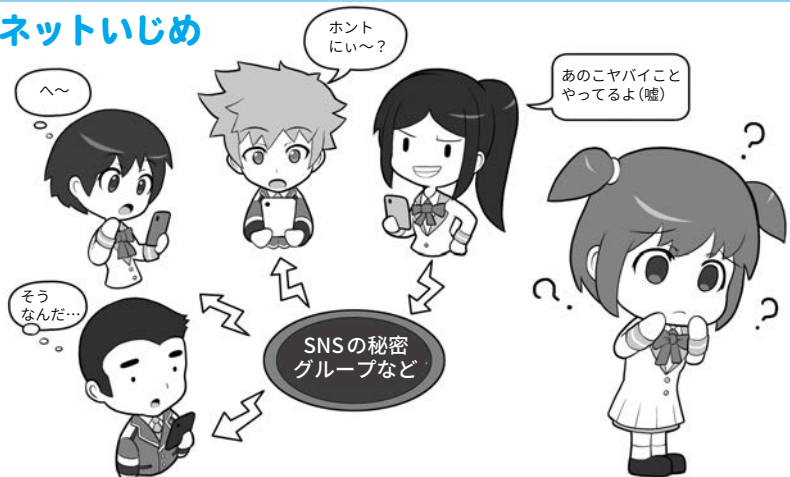
SNSなどであなたに近寄るために、年齢や性別を偽っている人がいます。同じ歳や性別になりすまし油断させて近づき、誘い出して誘拐や略取に及ぶかもしれません。基本的に実際に会ったことがない人がSNSで近づいてきたら、「そういう人かもしれない」と考え安易に信用しないようにしましょう。

### 自画撮り(セクスティング)被害



「自画撮り（セクスティング）」被害は、裸の写真などを送ってしまうことで起こります。もしその相手が写真をネットで売ったり、写真を使ってさらにあなたを脅したりしたらどうでしょう。一度ネットに流出した写真は完全に消し去ることは困難です。絶対にやってはいけません。

### ネットいじめ



現実のいじめはもちろんのこと、ネットを使ったいじめもやってはいけません。ネットはみんなの未来を創るためのものであって、苦しめるためのものにしてはいけないのです。

**各章ダイジェスト****プロローグ****インターネットにある基本的な  
リスクやトラブルを知ろう**

私たちは、スマホやパソコンを用いて、いつでもどこでもインターネットにつながり、便利なサービスを利用したり、世界中の人とコミュニケーションしたりできます。しかしインターネットには、注意したいリスクやトラブルがあります。まずは本書全体を通じて登場する基本的なリスクやトラブルについて知りましょう。

→P.13～26

**第1章****まずはサイバーセキュリティの  
基礎を固めよう**

サイバー攻撃を受けないようにするため、まずは基礎的なセキュリティの固め方を理解しましょう。スマホやパソコンを最新の状態にすること、安全なパスワードの管理方法、もしものときのバックアップの必要性など、攻撃する側からのサイバー攻撃を防ぐためにはどうすればよいかを学びましょう。

→P.27～48

**第2章****よくあるサイバー攻撃の手口や  
リスクを知ろう**

基礎的なセキュリティを固めても、インターネットにつながる限りサイバー攻撃を受けてしまうリスクはあります。実際にサイバー攻撃を受けてしまうとどんな被害があるのでしょうか。乗っ取りやランサムウェアなど、よくある被害について学びましょう。

→P.49～56

**第3章****SNS・ネットとの付き合い方や  
情報モラルの重要性を知ろう**

現代では、SNSを通じて、世界中の人たちと簡単につながりコミュニケーションできます。しかし、接する人がすべて自分と友好的であるとは限りません。SNSやネットでよくある危険やトラブルについて知り、対策や家族を守る方法を学びましょう。

→P.57～78

**第4章****災害・テロ、海外でのトラブル、  
普段とは違う環境のリスクに  
備えよう**

災害・テロなど、非常時にもインターネットにつながり情報収集することは大切です。また、海外でインターネットを利用する際、日本では遭遇しないトラブルやリスクがあります。普段とは違う環境に備えるには、普段からどんな準備をしておくとういかが学びましょう。

→P.79～90

**第5章****スマホやパソコン、IoT機器を  
安全に利用するための  
設定を知ろう**

スマホ・パソコンを中心に、安全を守るための設定について学びましょう。またIoT機器ならではの注意したいリスクについても解説します。どのように情報を守るか、どのように安全にインターネットを利用するか、具体的な設定方法を学び不安なく利用できるようにしましょう。

→P.91～108

**第6章****パスワードの大切さを知り、  
通信の安全性を支える暗号化に  
ついて学ぼう**

インターネットを安全に利用するには適切なパスワード管理が不可欠です。また通信の安全性を保つには暗号化技術が役立っています。パスワード管理、知っておきたい暗号化の必要性やしくみを学びましょう。

→P.109～148

**第7章****中小組織向け  
セキュリティ向上が利潤追求に  
つながることを理解しよう**

人材・体制・資金などが限られた中小企業にとって、通常業務をこなしながらセキュリティ対策を講じるための負担は少なくありません。しかし、企業経営においてセキュリティ対策を省くことはできません。セキュリティ対策に投資すべき理由、テレワークを安全快適に利用するために必要なルール作り、企業だからこそ気を付けたいサイバー攻撃、そして最低限把握しておきたいセキュリティ関連の法律などを学びましょう。

→P.149～172

**付録****知っておくと役立つサイバー  
セキュリティに関する  
手引き・ガイダンス**

本書の最後には、知っておくと役立つ手引きやガイダンスなどを紹介します。サイバー攻撃を受けた場合に相談できる公的機関の窓口、スキルアップしたい中小組織のセキュリティ部門担当者役に役立つ情報、そして本格的な普及がはじまったマイナナンバーカードなど、実践的な内容を解説します。また、本章では、「一般国民向け」「中小組織向け」と中心となる対象読者を表すタグを付しています。

→P.173～188

## サイバーセキュリティ対策9か条

次のP.27からはじまる第1章より、NISCとIPAが提唱する「サイバーセキュリティ対策9か条」に即した、基本的なセキュリティの考え方・対策を解説します。

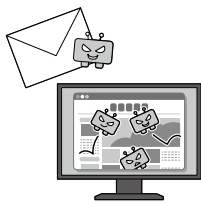
### 2 パスワードは長く複雑にして、 他と使い回さないようにしよう



yC.qk2,ehgMG  
\$ZJBSFvT&+Bj

パスワードは長く複雑にし、機器やサービス間で使い回さないことを徹底して安全性を高めましょう。

### 4 偽メールや偽サイトに 騙されないように用心しよう



フィッシング詐欺メールは年々手口が巧妙になっています。心当たりがあるものでもメールやメッセージのURLには安易にアクセスしないようにしましょう。

### 6 スマホやPCの画面ロックを 利用しよう



スマホやパソコン(PC)の情報を守るには、まず待ち受け画面をロックすることが第一です。短時間であっても端末を手元から離す際はロックを忘れないようにしましょう。

### 8 外出先では紛失・盗難・ 覗き見に注意しよう



外出先でスマホやパソコンを使うときは、背後からの覗き見に注意しましょう。また、紛失・盗難の危険があるので、公共の場でスマホを放置することは絶対にやめましょう。

### 1 OSやソフトウェアは 常に最新の状態にしておこう



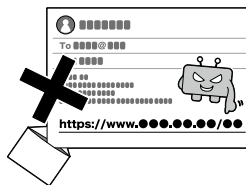
最新の攻撃情報に対抗するため、OSやソフトウェアメーカーが提供している修正用アップデートを常に適用しましょう。

### 3 多要素認証を利用しよう



サービスへのログインを安全に行うために、認証用アプリや生体認証を使った多要素認証を利用しましょう。

### 5 メールの添付ファイルや 本文中のリンクに注意しよう



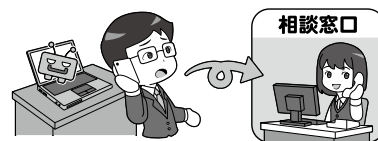
心当たりのない送信元からのメールに添付されているファイルやリンクはもちろん、ファイルやリンクを開かせようとするものには注意しましょう。

### 7 大切な情報は失う前に バックアップ(複製)しよう



大切な情報を失っても、バックアップから復元することで被害を軽減することができます。普段からバックアップして攻撃や天災に備えましょう。

### 9 困ったときは1人で悩まず、 まず相談しよう



インターネットでの被害に遭遇したら、1人で悩まず各種相談窓口にご相談しましょう。

## 第1章

# まずはサイバーセキュリティの基礎を固めよう

サイバー攻撃を受けないようにするため、まずは基礎的なセキュリティの固め方を理解しましょう。スマホやパソコンを最新の状態にすること、安全なパスワードの管理方法、もしものときのバックアップの必要性など、攻撃する側からのサイバー攻撃を防ぐためにはどうすればよいかを学びましょう。

### 1 最低限実施すべきサイバーセキュリティ対策を理解しよう

#### 2 ①OSやソフトウェアは常に最新の状態にしておこう

- 2.1 パソコン本体とセキュリティの状態を最新に保とう
- 2.2 スマホやネットワーク機器も最新に保とう

#### 3 ②パスワードは長く複雑にして、他と使い回さないようにしよう

- 3.1 パスワードの安全性を高める
- 3.2 機器やサービス間でのパスワード使い回しは「絶対に」しない
- 3.3 パスワードを適切に保管する

#### 4 ③多要素認証を利用しよう

- 4.1 可能な限り多要素や生体認証を使い、秘密の質問にはまじめに答えない
- 4.2 パスワードはどうやって漏れるの？どう使われるの？

#### 5 ④偽メールや偽サイトに騙されないように用心しよう

- 5.1 多様化する偽メールに注意しよう
- 5.2 公式サイト以外からアプリをインストールすることは控えよう

### 6 ⑤メールの添付ファイルや本文中のリンクに注意しよう

#### 7 ⑥スマホやPCの画面ロックを利用しよう

- 7.1 スマホやパソコンには必ず画面ロックをかけよう
- 7.2 よくある情報の漏れ方と対策

#### 8 ⑦大切な情報は失う前にバックアップ(複製)しよう

- 8.1 何をするにもバックアップを取ろう
- 8.2 ランサムウェアや天災にも対応できるバックアップ体制

#### 9 ⑧外出先では紛失・盗難・覗き見に注意しよう

#### 10 ⑨困ったときは1人で悩まず、まず相談しよう

- コラム.1 攻撃されにくくするには、手間(コスト)がかかるようにする
- コラム.2 利益が目的ではない攻撃に備えるには
- コラム.3 セキュリティソフトを導入しても過信しないことが重要



## 1

# 最低限実施すべきサイバーセキュリティ対策を理解しよう

攻撃者▶用語集 P.196 (悪意のハッカー▶用語集 P.193) による攻撃を防ぐには、まずはパソコンやスマホの基本的なセキュリティを固め、また、トラブルが発生したときの対処手段を知ることが重要です。

現在、政府系機関が掲げるサイバーセキュリティ対策の指針としては、NISC▶用語集 P.191 (内閣官房内閣サイバーセキュリティセンター▶用語集 P.200) が「サイバーセキュリティ対策9か条」を公開しています。一般国民の誰もが最低限実施すべき対策をまとめており、本ハンドブックもこの9か条に則ってサイバーセキュリティ対策を解説していきます。

まず「①OSやソフトウェアは常に最新の状態にしておこう」はいわゆるアップデート▶用語集 P.194 のことです。IT機器にはセキュリティホール▶用語集 P.198 と呼ばれる弱点が日々見つかっています。一見、大丈夫そうに見えてもそれは「ただセキュリティホールが発見されていない」だけ。OS▶用語集 P.191 やソフトウェアメーカーが提供している修正用アップデートを常に適用し続け、攻撃の糸口となる穴を塞ぎます。

「②パスワードは長く複雑にして、他と使い回さないようにしよう」は、安全性の高いパスワード▶用語集 P.200 を設定する際の留意点、同じパスワードの使い回しの危険性、パスワードの適切な管理方法について解説します。

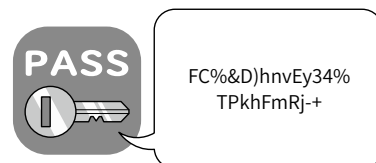
「③多要素認証を利用しよう」は、

## ①OSやソフトウェアは常に最新の状態にしておこう



OSやソフトウェアを最新に状態にする理由は、最新の攻撃情報への対策が盛り込まれているからです。

## ②パスワードは長く複雑にして、他と使い回さないようにしよう



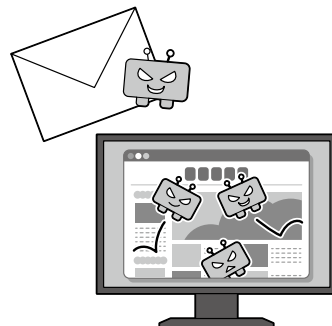
安全なパスワードの作成方法はもちろん多要素認証の重要性を説明します。

## ③多要素認証を利用しよう



認証用アプリや生体認証を利用したより安全性の高い多要素認証について説明します。

## ④偽メールや偽サイトに騙されないように用心しよう



多様化・複雑化するフィッシング詐欺メールや、公式サイト以外からアプリをインストールする危険性について解説します。

サービスへのログイン▶用語集 P.204 を安全に行うために、二要素以上を使って認証作業をする多要素認証▶用語集 P.198 について解説します。認証用アプリや生体認証▶用語集 P.198 を利用するとログインの安全性を高められます。

「④偽メールや偽サイトに騙されないように用心しよう」は、フィッシング詐欺メールが多様化しており攻撃が複雑になっていることや、公式サイト以外からアプリ▶用語集 P.194 をインストール▶用語集 P.194 する危険性を解説します。



「⑤メールの添付ファイルや本文中のリンクに注意しよう」は、近時また猛威を振るう「Emotet」のように、マルウェア▶用語集 P.203 添付メールで広がる感染、標的型メール▶用語集 P.201 やスパムメール▶用語集 P.197 の実例を挙げ、具体的リスクについて解説します。

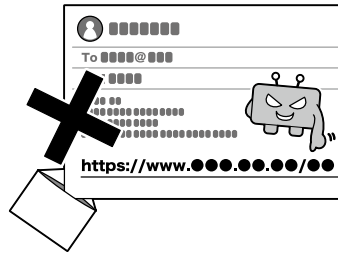
「⑥スマホやPCの画面ロックを利用しよう」は、スマホやパソコン(PC)の情報を守るにはまず待ち受け画面をロック▶用語集 P.204 することが第一であることを解説します。また、生体認証を使用したロックの利点や、安易に他人へ端末を渡す危険性についてもふれます。

「⑦大切な情報は失う前にバックアップ(複製)しよう」は、普段からバックアップ▶用語集 P.201 をとっておくことがどれほど重要か解説します。正常な状態のファイルをバックアップして保管しておくことで、仮に攻撃を許して重要なファイルを失っても、バックアップから復元▶用語集 P.202 することにより、被害を軽減します。とくに昨今増加しているランサムウェア▶用語集 P.203 攻撃に対してもバックアップを準備しておくことは有効です。

「⑧外出先では紛失・盗難・覗き見に注意しよう」は、勤務先や外出先でスマホやパソコンを使う際、覗き見されるショルダーハッキング▶用語集 P.197 などのリスクなどについて解説します。また、飲食店などで離席時に端末を置いていく人を時折見かけますが非常に危険な行為です。公衆の場でスマホやパソコンを利用するときに注意すべきことについて把握しましょう。

「⑨困ったときは1人で悩まず、まず相談しよう」は、サイバー攻撃▶用語集 P.196 などインターネットの被

## ⑤メールの添付ファイルや本文中のリンクに注意しよう



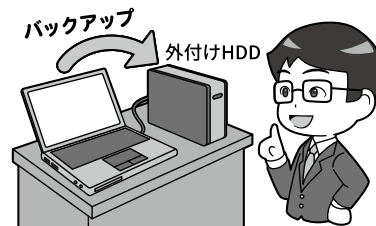
被害がなくなる「Emotet」、標的型メール、スパムメールの実例を紹介

## ⑥スマホやPCの画面ロックを利用しよう



スマホやパソコン(PC)の情報を守るにはまず待ち受け画面をロックすることが第一。そして生体認証が推奨

## ⑦大切な情報は失う前にバックアップ(複製)しよう



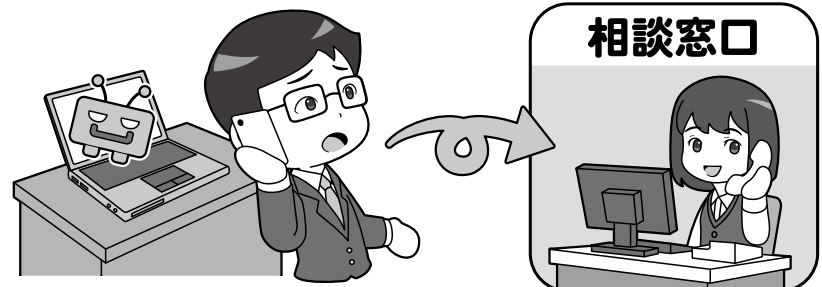
たとえ攻撃されても、適切にバックアップしておけば、すぐに復旧できます。

## ⑧外出先では紛失・盗難・覗き見に注意しよう



公衆の場における、ショルダーハッキングのリスク、スマホやパソコンの紛失・盗難など、利用時の注意すべきことを把握しましょう。

## ⑨困ったときは1人で悩まず、まず相談しよう



攻撃されたとき、どうしたらよいかわからないからそのまま放置せず、相談窓口相談しよう。また、実質的な被害が出ている場合は、警察などの関係機関に報告した方がよい場合もあります。いざというとき慌てないように、あらかじめ連絡先を調べておきましょう。

害で自分だけでは対処できないときには、積極的に警察やIPAなどの窓口へ相談する重要性を解説します。

あらかじめ窓口を調べておくことで、困ったときにすぐに相談できるようになります。

\*「サイバーセキュリティ対策9か条」<https://www.nisc.go.jp/pdf/council/cs/jinzai/dai17/17shiryou0101.pdf>

# ① OSやソフトウェアは常に最新の状態にしておこう

## 2.1 パソコン本体とセキュリティの状態を最新に保とう

悪意の攻撃からパソコンを守る第一歩は、セキュリティを最新に保ち、各種のアップデート(バージョンアップ▶用語集 P.200)を行うことです。

最近の機種では、OS関連のアップデート処理は自動で行われるか、アップデートを行うよう通知が出ています。しかし、緊急でアップデートを行った方がよいときもあります。セキュリティ関連ニュースサイトなどでアップデートを促す情報が流れていたら、自主的に更新処理をかけるようにしましょう。Office製品▶用語集 P.191 などOSのメーカーが作っている重要なソフトもここで同時にアップデートします。

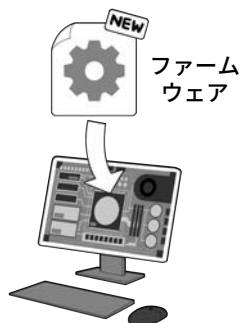
次に、サイバー攻撃で狙われやすいソフトウェアの更新を重点的に行いましょう。Adobe社 Acrobat Reader や Oracle 社 Java、そして Google Chrome をはじめとする各種のウェブブラウザ▶用語集 P.195 は攻撃のターゲットになりやすいのです。

また、機器そのものの基本プログラムを更新するファームウェアアップデートにも気を配りましょう。こちらの更新通知は、自動で出る機器と出ない機器があるので、自分の機器用のアップデート情報は、どのようにすれば入手できるか、事前に確認して気を配ってください。

セキュリティソフト▶用語集 P.198 をインストールしている場合は、最新のウイルス定義ファイルに自動更新されるよう設定しておきましょう。

### 本体も OS もセキュリティソフトも重要ソフトもアップデート

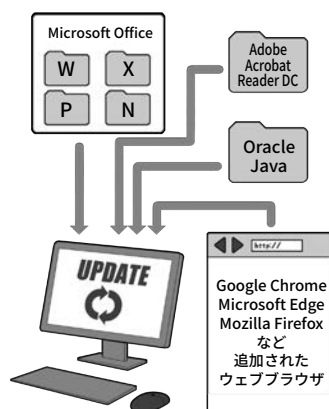
#### 本体のファームウェアも更新



#### OS と基本ソフトの更新



#### 重要ソフトも更新



#### セキュリティソフトも更新



OS やファームウェアなどは、社会でいえば鉄道や電気ガス水道のような社会インフラに相当し、そのためほとんどのパソコンで利用されています。

利用する側もアップデート(更新)が必要になれば速やかに適用して、攻撃者が攻撃できないようにしましょう。インストールしてあるが使っていない重要ソフトは削除(アンインストール▶用語集 P.194)してしまってもよいでしょう。

ボットネット▶用語集 P.203 も、そもそも攻撃して乗っ取れる機器がなければ成立しないように、攻撃できる穴を作らない1人1人の行動が、安全なインターネットを作り社会インフラを支えるのです。

なお、OS やソフトウェア、ファームウェア▶用語集 P.201 は、開発者がアップデートの期限を設定しているものが多く、この期限を過ぎるとアップデートが提供されなくなります。

アップデートが提供されなくなっ

たOS やソフトウェアは、セキュリティホールが見つかって修正用アップデートが提供されず、攻撃に対して非常に脆弱なので、使用しないようにしてください。

## 2.2 スマホやネットワーク機器も最新に保とう

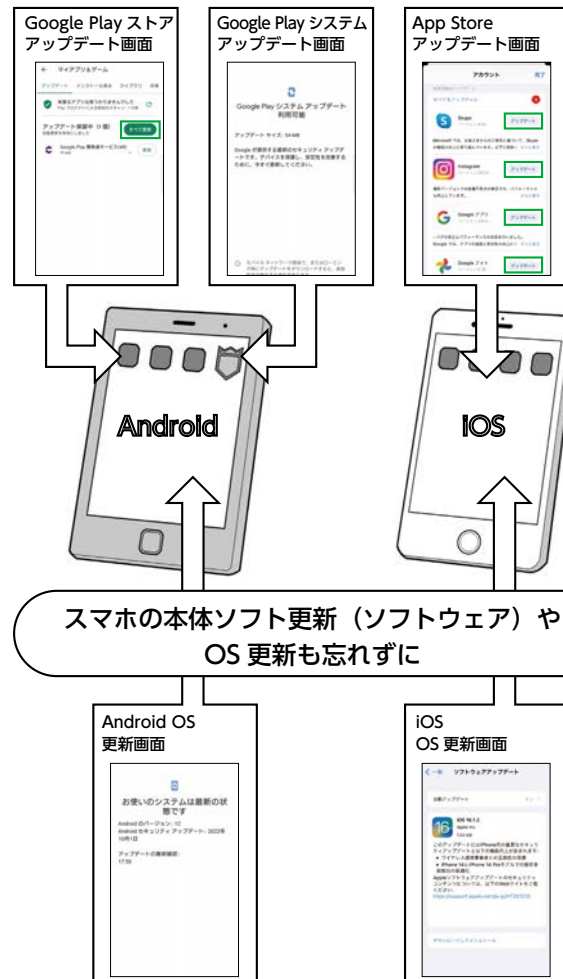
スマホも同様に各種のアップデートの適用が必須です。スマホの場合、比較的アップデートの通知がわかりやすくなっており、自動アップデート機能も充実しています。機器本体のファームウェアのアップデートでも、OSのアップデートでも、いつも使用している一般のアプリのアップデートでも、更新の通知が出たら、マメに適用するようにしましょう。そのためには、本体のファームウェア(ソフトウェア更新やシステムアップデートと書かれることも)やOSの更新が、設定メニュー上のどこにあるのかと、更新の手順を確認しておきましょう。アプリの更新が自動になっているかも確認しましょう。

スマホアプリの自動更新は、設定によっては無線LAN▶用語集 P.203 接続時のみ自動で行うことになっている場合もありますが、その設定でも更新時に権限変更で確認が必要な場合は自動更新されないこともあるので、気が付いたら未更新のアプリがたくさんたまってしまうこともあります。日に一度は意識してアップデート画面に行き、更新作業をするように心がけましょう。

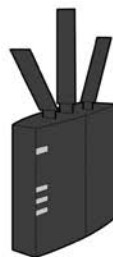
また、ネットワークにつながるルータやIoT機器、スマート家電▶用語集 P.197 など脆弱性を狙った攻撃の対象となるため、ファームウェアが自動更新されるよう設定しておきましょう。2022年以降国際情勢の影響もあり、更新されていないネットワーク機器を狙う攻撃が増加しました。

ルータはここ数年で自動更新機能搭載のものが普及してきているので、可能であれば買い換えましょう。

### アプリやセキュリティソフトの更新は自動更新にしつつ、まめにチェック



### ネットにつながるIT機器(ルータやIoT機器)もファームウェア更新や管理者用初期IDとパスワードの変更をしておくこと



無線LAN アクセスルータ



ネットワーク対応プリンタ



ネットワークカメラ

▶用語集 P.200

IoT機器のファームウェアの更新は、通常はウェブブラウザで本体にアクセスして行います。このときの管理者用IDとパスワードは、必ず購入時の初期のものから変更しておきましょう。同じ機種で共通だった場合など、不正アクセスされ乗っ取られてサイバー攻撃に使われます。

## ②パスワードは長く複雑にして、 他と使い回さないようにしましょう

### 3.1 パスワードの安全性を高める

サイバー攻撃には、相手の機器をマルウェアに感染させて乗っ取る方法の他に、なんらかの手段でID▶用語集 P.191 とパスワードを解明し、サービスや機器を乗っ取る方法もあります。

パスワードは利用しているウェブサービスなどから大量流出したものが使われる「リスト型攻撃▶用語集 P.203」、文字の組み合わせをすべて試す「総当たり攻撃▶用語集 P.198」、パスワードによく使われる文字列を利用する「辞書攻撃▶用語集 P.197」などにより探し当てる方法や、IoT 機器のパスワードを購入時のまま利用していると乗っ取られることもあります。総当たり攻撃を防ぐには、探し当てるまでに膨大な時間がかかるようにするのが一番の防御手段で、それには1桁の文字の種類と桁数による組み合わせを増やします。例えば数字だけなら1桁10通りしかありませんが、英字を入れると36通り、

#### ログイン用パスワードは英大文字小文字+数字+記号で10桁以上

「ログインに使うパスワードは、英大文字小文字+数字+記号で10桁以上」の理由

「数字のみ」の10乗だと→100億通り

(英大文字小文字+数字+記号(88個として))の10乗だと→  
約2785京97兆6009億通り

数字だけで10桁と、英大文字小文字+数字+記号で10桁では雲泥の差がある。  
そしてこれほど多量な組み合わせは、機械入力でも事実上突破不可能。

#### 英大文字小文字+数字+記号混じりの組み合わせ数

アルファベット(大)+アルファベット(小)+数字+記号(例)

26 + 26 + 10 + 26 = 88

数字	英大文字	英小文字	記号	合計	5	6	7	8	9	10
10			10	数	100,000	1,000,000	10,000,000	100,000,000	1,000,000,000	10,000,000,000
10	26		36	数英	60,466,176	2,176,782,336	78,364,164,096	2,821,109,907,456	101,559,956,668,416	3,656,158,440,062,976
10	26	26	62	数英大小	916,132,832	56,800,235,584	3,521,614,606,208	218,340,105,584,896	13,537,086,546,263,552	838,299,365,868,340,224
10	26	26	26	数英大小記	5,277,319,168	464,404,086,784	40,867,559,636,992	3,596,345,248,055,296	316,478,381,828,866,048	27,850,097,600,940,212,224

英大文字小文字を入れると62通り、これに26文字の記号を入れると約88通りになります。これに桁を増やして、累乗で組み合わせを増やすわけです。総当たり攻撃は、理論上攻撃し続ければいつかは成功するのですが「時間がかかり事実上不可能な状態」にして防ぐのです。長いが覚えやすいパスワードにするか、短

いが複雑なパスワードにするかは、好みの問題ともいえますが、ログイン用パスワードであれば入力ごとに遅延がかかるので、英大文字小文字+数字+記号混じりで10桁以上を安全圏として推奨します。しかし、より組み合わせ数を増やし安全性を高めるにこしたことはありません。

### 3.2 機器やサービス間でのパスワード使い回しは「絶対に」しない

複雑なパスワードを使っても、それを複数のサービスや機器の間で使い回していれば意味がありません。1カ所から漏れればすべてログイン可能になってしまうからです。複雑なパスワードを1つ決めて、あとはおしりに数字や規則性のある文字を付けるのも、2つ以上漏れれば推測されます。それぞれに複雑なパスワードを設定し、使い回しをしないことが大切です。

#### 同じパスワードを使い回さない。似たパスワード、法則性のあるパスワードも×



	白うさネットワーク	おさるさん銀行	三毛猫電気	たこクレジット	
×使い回し	PASSPPOI	PASSPPOI	PASSPPOI	PASSPPOI	1個漏れたら一網打尽
×おしりだけ違う	PASSPPOI1	PASSPPOI2	PASSPPOI3	PASSPPOI4	推測しやすい
×法則性あり	USAGIPPOI	OSARUPPOI	NEKOPPOI	TACOPPOI	法則性がばれたらおしまい



### 3.3 パスワードを適切に保管する

使い回しをせず十分な複雑さと長さを持ったパスワードは、総当たり攻撃では突破されにくくなります。しかし、適切に管理しておかず、別の方法で盗まれてしまってはひとたまりもありません。

例えばパソコンや壁に貼ってあれば、誰かがそれを見て覚えてしまいますし、テキストファイルにまとめておけばマルウェアに感染したときに流出し、多くのアカウントが一気に乗っ取られるかもしれません。

パソコンでウェブブラウザにパスワードなどを覚えさせる「自動入力」機能も要注意です。あなたが席を離れた際に、誰かがブラウザ▶用語集 P.202 でウェブサービスを利用してしまいかもしれません。それにノートパソコンならば本体ごと盗まれることもあります。パスワードは基本的に利用する場所で保管してはいけません。

しかし、多くのサービスで複雑なパスワードをそれぞれ設定したら、とても覚えきることはできません。ではどうしたらよいでしょう。

1つは、パスワードを管理する紙のノートに書いてパソコンとは別に保管する方法。もう1つはスマホのパスワード管理アプリ▶用語集 P.200 を利用する方法です。なお、後者の場合、クラウド▶用語集 P.195 でデータを保管する機能の利用は熟考し、過去に情報流出にまつわるトラブルのあったアプリやサービスは利用を避けるようにしましょう。それは他人の手元にIDやパスワードを保管することや、流出の危険が逆に増すことを意味するからです。

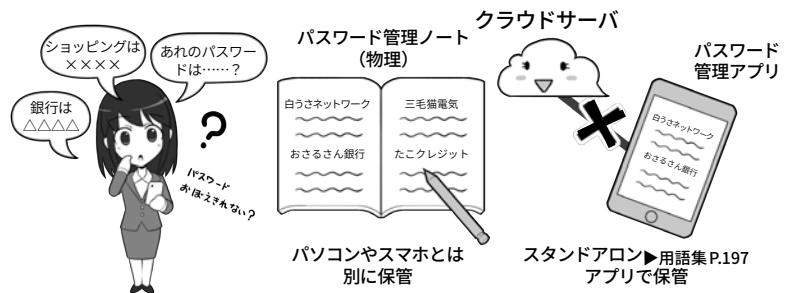
利用するところで保管するべきで

#### パスワードを使用する場所に置かない。パソコンの中も×



オフィスの中ならば外の人は見ないと判断するのは×。出入りの業者が見たり、外から双眼鏡で見たりすることもできるのです。内部の人間が勝手に使うリスクもあります。

#### パスワードは紙のノートに書いて保管するか、パスワード管理アプリで守る



クラウド保管＝ダメというわけではなく、それは利便性との兼ね合いです。アプリのバグや過去のトラブルは、アプリ名＋「トラブル」などで検索します。

#### ウェブブラウザの自動入力にパスワードを覚えさせない



パスワードなどの自動入力は便利ですが、仕事場などであなたがパソコンをロックしないまま席を離れると、他人が各種サービスにログインし放題になります。

ないなら、スマホでパスワードを管理する場合リスクはありますが、こういったアプリは後述のPINコード▶用語集 P.191 (P.110 参照) や指紋認証＋暗号化▶用語集 P.194 で情報がガードされます。盗まれても落としても、簡

単に他人が使ったりすることはできません。

ただ、管理しているパスワードは、必ずバックアップするのを忘れないようにしましょう。落としたスマホが戻るとは限りませんから。

## ③多要素認証を利用しよう

### 4.1 可能な限り多要素や生体認証を使い、秘密の質問にはまじめに答えない

サービスへのログインを安全に行うために、二要素以上を使って認証作業をする多要素認証などの方法が提供されていれば必ず設定しましょう。これらの方法では通常のパスワードの他に、使い捨てにする別のパスワードを、ハードウェアトークン▶用語集 P.200 や生成アプリで作り、ログイン時に利用者に入力させます。メールやSMS▶用語集 P.192 ・ショートメッセージを利用する方式もありますが、これらは安全面で非推奨です。

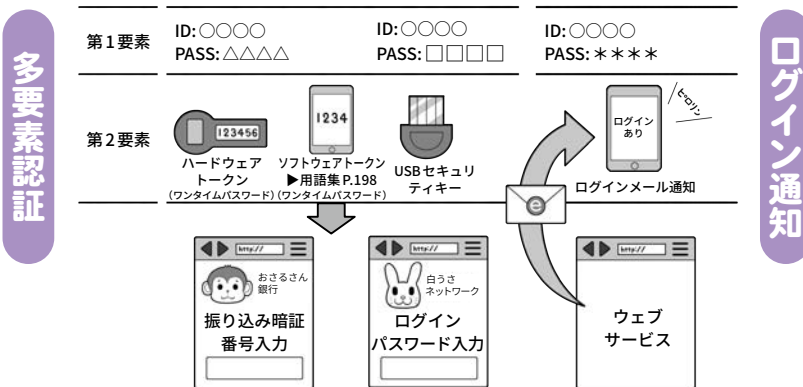
その他にも、USBセキュリティキー▶用語集 P.193 などを利用者を確認する方法や、不正アクセス▶用語集 P.202 の兆候を知る手段として、サービスに不審なログインがあったときにメールで利用者に通知を送る機能も存在するので、あれば活用しましょう。

また、最近の機器では顔、虹彩▶用語集 P.196、指紋で本人確認をして機器のロック状態を解く、生体認証機能もあります。

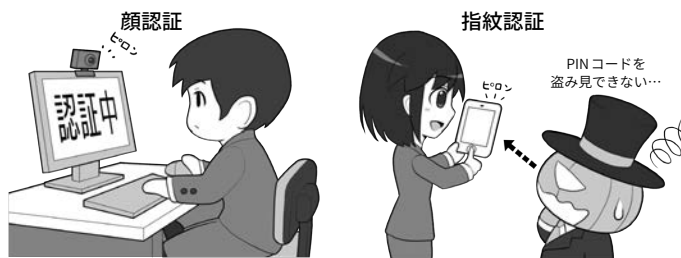
生体認証は本人のみが使って安全性が高く、肩越しの盗み見などによる暗証番号(PINコード)の盗難には強い機能でもあります。ただ指紋認証などは寝ている間に勝手にロック解除されることがあり得るので過信は禁物です。

なお、生体認証はたいていは通常のPINコードの替わりなので、スマホでは失敗すると通常のPINコード入力に戻ります。誕生日などの個人情報▶用語集 P.196 をPINコードにする

#### 多要素認証やログイン通知でセキュリティを向上



#### 生体認証を使う



と予想がされやすく、本体を盗まれてロック解除される可能性が上がるため使わないようにしましょう。

その他、認証システムによっては、スマホなどへのプッシュ通知を多要素認証に組み入れることがあります。攻撃者がパスワードなどでの認証を成功させた場合にもプッシュ通知が送られるので見知らぬプッシュ通知には回答してはいけません。

その他のウェブサービスの中には、パスワードを忘れてしまった場合や、あるいはいつもと違うログインがあった場合の本人確認のために「秘密の質問」▶用語集 P.201 と呼ばれる機能で対応しようとするものがあります。こ

れはあらかじめ利用者が、自分しか知らない質問と答えを設定しておいて、合い言葉的にこれに答え、本人であることを証明するものです。

しかしこの秘密の質問は、自分で質問を作るものもありますが、多くは「生まれた市は」「ペットの犬の名前は」と回答が類推しやすいものが大半です。

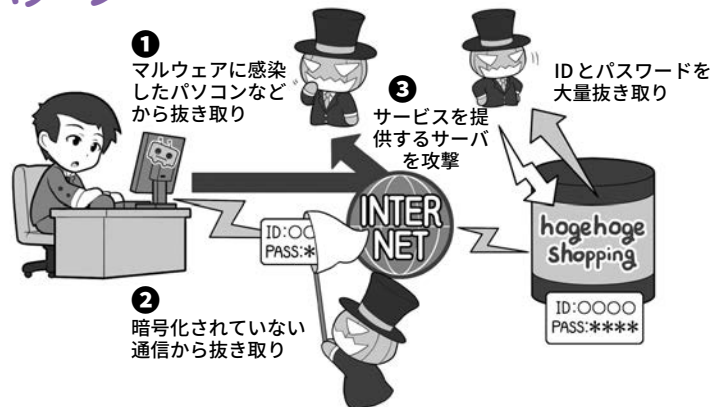
SNS▶用語集 P.192 が普及した今、ネット上で簡単に見つけられることもあり、安全性が高いとはいえません。秘密の質問に答えを設定する場合は推測できないものにし、忘れないようにパスワード管理アプリなどに保存しましょう。

## 4.2 パスワードはどうやって漏れるの？ どう使われるの？

### さまざまなIDとパスワードの漏えいパターン

攻撃者にIDとパスワードが漏えいする事態は、機器がマルウェアに感染したり、自分が通信する過程で抜き取られたりする他に、利用しているサービス側からも流出するケースもあります。

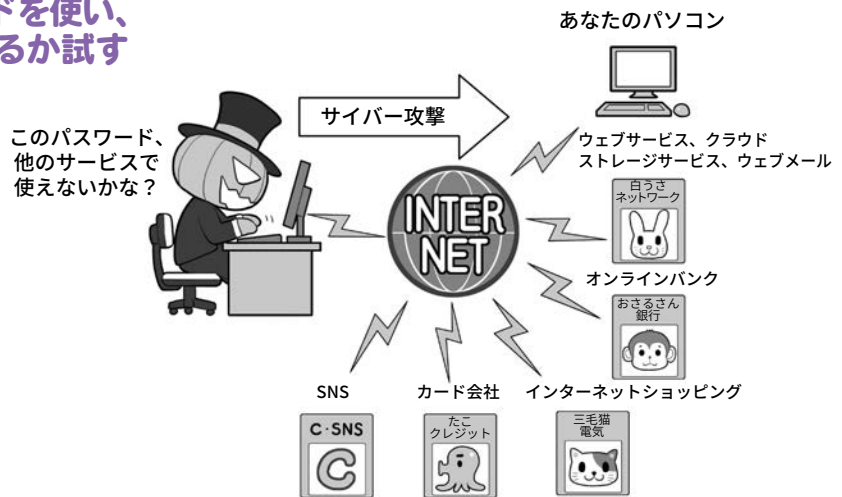
ニュースや通知でサービス側から流出が判明した場合は、速やかにパスワードを変更するなどの対応を取りましょう。



### 攻撃者は入手したIDとパスワードを使い、さまざまなサービスを乗っ取れるか試す

IDとパスワードをなんらかの手段で手に入れた攻撃者は、これをどこか別のサービスで使えないかさまざまな方法で試します。

こういった攻撃を成功させないために、パスワードの使い回し▶用語集 P.201や、似たパスワード、パターンのあるパスワード、個人情報などから推測できるパスワードを利用するのはやめましょう。



私たちがパソコンやスマホ、あるいはSNSやウェブ上のサービスを利用するときに入力するIDやパスワード。サイバー攻撃でこれらの情報を盗まれると、かなり深刻な被害を起こしかねないものです。

では実際はどのように漏れてしまうのでしょうか？

1つには、自分のパソコンなどがマルウェアに感染し、そのマルウェアがパスワードを盗み取って攻撃者に送信するケース。次に、ウェブサービスなどにログインするときに、私たちが利用する機器からウェブサービスまでの経路上のどこかで盗み取られてしまうケース。そして、ウェブ

サービス側でログインを認証するために控えとして持っているIDやパスワードが、攻撃者によって盗み取られ漏れいするケースなどがあります。

先ほど説明しましたが覚えておいてほしいのは、自分がマルウェアなどに感染していなくても、漏れてしまうケースがあるということです。したがってIDやパスワードを普段入力していないから安心、とも言いきれません。

そしてIDとパスワードを盗み取った攻撃者は、それを使ってどこか別のウェブサービスなどが乗っ取れないか、さまざまな場所で試します。

あなたが複数のウェブサービスの間でIDとパスワードを使い回していたり、あるいは似た形のパスワードを使ったりしていると、これらのサービスのアカウントを一気に乗っ取られます。

乗っ取られると、あとはオンラインショッピングで勝手にものを買われてしまったり、現金は送れなくてもなんらかの送金システムが利用できる場合は、それを使ってお金を奪い取られたりされてしまうわけです。

もしパスワード流出が判明したら、まずはすぐにパスワードを変更しましょう。

## ④偽メールや偽サイトに騙されないように用心しよう

### 5.1 多様化する偽メールに注意しよう

サイバー攻撃を行う際に、攻撃者は偽メール、偽サイトを使うことが多いです。これは、攻撃者からしたら攻撃のためのコストを低く抑えられるためです。

偽メールには、スマホ宛の偽SMSやSNSで使用可能なメッセージ機能なども含みます。

近年、フィッシング詐欺の攻撃で最も目を引いたのは、宅配業者の不在通知詐欺です。宅配業者を名乗って「配達に行ったが不在だった。下記のリンク▶用語集 P.204 から確認してほしい」というようなSMS(ショートメッセージ)を送り付けて、利用者をリンク先の偽サイトに誘導し、そこでIDとパスワードなどを詐取するというものです。

実は、この業者は「SMSで不在通知を行わない」のですが、それを知らない人たちはまんまとだまされてしまったわけです。関係機関で日々、「不審なメールに気を付けてください」というアナウンスをしているのですが、SMSとメールは違うものと思われてしまったのかもしれない。

偽メールについても、国税庁を装ったりETCサービスを装ったりと、騙られる送信元にバリエーションが増えてきていますが、偽メールであることには間違いありません。またこういったメッセージを使った詐欺には、SMSやメールだけでなく、SNS

#### フィッシング詐欺はいろんな方法がある

##### SMS(ショートメッセージ)



電話番号宛てに送る

##### 電子メール(eメール)



メールアドレス宛に送る

##### メッセージ(アプリなど)



アプリのアカウント宛に送る

##### ゲーム内のメッセージ機能



ゲームのユーザー宛に送る

「怪しいメール」といわれたら「メール」だけでなく似たような機能全般に気を付けましょう。

#### 驚くと人間は警戒心を忘れる



災害時などに驚いて人間の警戒心が弱くなった瞬間を狙った攻撃もあります。注意しましょう。

フィッシング対策協議会 <https://www.antiphishing.jp/>  
内閣サイバーセキュリティセンター Twitter @nisc\_forecast

のメッセージ機能、あるいはゲーム内のメッセージ機能を使った攻撃も実際に発生していますので、偽メー

ルと同様に注意してください。心当たりのないものは無視し、心当たりがあるものでも、そのメールやメッ



ページの URL ▶用語集 P.193 などアクセスするのではなく、後述するような対処を行ってください。

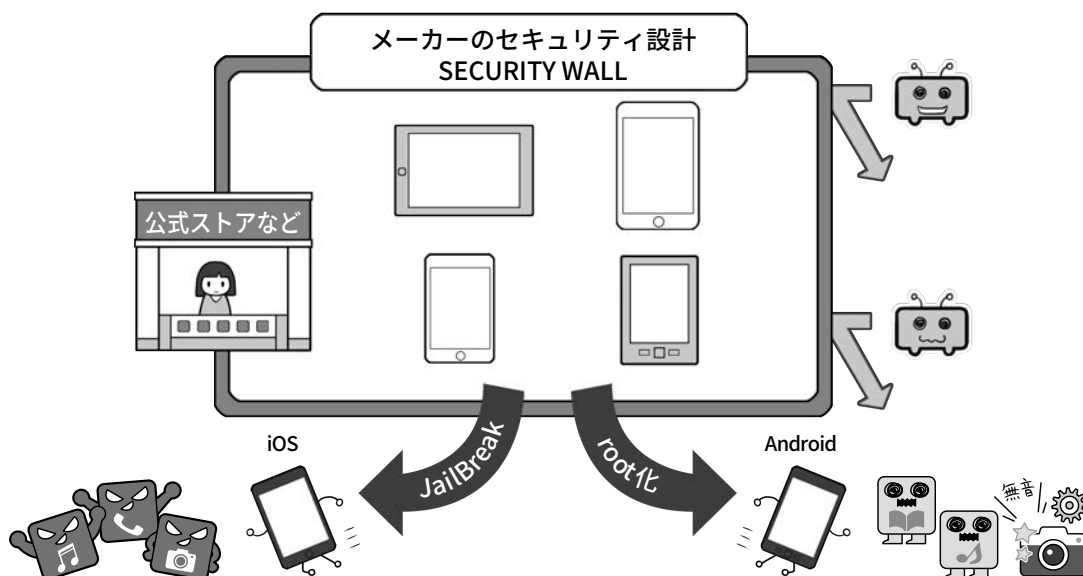
他にも、地震が発生したときに、気象庁を名乗って津波に関する迷惑メール ▶用語集 P.203 が送られた例もありました。いずれも私たちが「だまされないぞ」と身構えているのとは違う方向や、災害時で正常な判断が行えない状況を狙っています。

こういった詐欺メールは年々手口が巧妙になっており、送信元アドレスやメッセージ中のリンクを確認しただけで、詐欺と見抜くことは極めて難しくなっています。基本は「見るだけで完結しない情報はすべて疑え」です。情報を確認する場合は、正規のウェブサイト ▶用語集 P.194 の URL を直接入力して見るか正規のアプリから行いましょう。

また、日々巧妙になる手口を少しでも知るにはフィッシング対策協議会 (<https://www.antiphishing.jp/>) のウェブサイトや内閣サイバーセキュリティセンターの Twitter (@nisc\_forecast) をフォローするとよいでしょう。最新の事例をすぐに確認できます。

## 5.2 公式サイト以外からアプリをインストールすることは控えよう

### サイドローディングやスマホの改造は控えましょう



スマホのセキュリティはメーカーが想定する利用方法を守っていることが前提条件です。非公式なアプリをインストールする「サイドローディング」は危険が伴う可能性がありますし、「root化」や「JailBreak」といった改造は規約違反である場合もあります。いずれもセキュリティ上、脆弱になるので非常に危険で、やっではないけません。

前項で紹介した偽メール、偽サイトの手法は多様化していて注意が必要ですが、スマホにインストールするアプリも同様に注意しなくてはなりません。

インストールしようとするアプリがどのような動作を行うものかをあらかじめ確認できればよいのですが、個人で、アプリの中身を分析し、不

審な動作などがされないことを確認することは簡単なことではありません。そのような確認作業を自分ではなく信頼できる第三者がしてくれれば少し安心できます。

公式ストアで配信されるアプリに関しては、公式ストアでの配信前にストア運営者が審査しているので一定程度のリスクは軽減されます。

公式のアプリストア以外のサイトからアプリをダウンロードすることを「サイドローディング」、さらに非公式なアプリのインストール以外にもスマホを標準にはない設定に変更できる改造を「root化」▶用語集 P.192 「JailBreak」▶用語集 P.191 と呼びますが、これらはセキュリティレベルを下げるためやっではないけません。

サイドローディングは、アプリをさまざまなサイトからインストールできることで企業間の競争が促進される可能性があるかもしれませんが、しかし、アプリの審査を行うためには、費用や時間・労力が必要です。何もチェックを行わず自由に公開を許すようなサイトよりは、運営費用がかかるのは当然で、そのようなコストが価格に反映される点も考慮する必要があります。またスマホの改造は規約違反になる場合もあり、セキュリティ上、脆弱になるので非常に危険です。

スマホには、個人に関する重要な情報がたくさん存在していますから、リスクの高いアプリをインストールし、重要な情報が漏えいしてしまうと、取り返しがつきません。アプリを利用する際には、安全を確保するためには一定の費用が必要なことと、アプリの審査を行っている信頼できるストアを使うという観点が不可欠です。

例えばスマホの場合、iOS 機器は公式のストア以外からはアプリを導入できない仕組みになっていますが、Android 機器の場合は公式ストアやベンダー▶用語集 P.202・メーカーのストア以外からもアプリをインストール可能です。それを利用し攻撃者がメールやSMSなどであなたを誘導して、公式ストアでない場所から不明なアプリ▶用語集 P.202をインストールさせ、端末を乗っ取ったり、端末内の情報を盗んだりする可能性があります。

Android 機器の場合、使用しているアプリで別のアプリをインストールする設定が最初からオフになっています。不明なアプリをインストールしないためにもこの設定はオフのままにしておくようにしましょう。

### 「不明のアプリ」という言葉に注意



#### ・Android

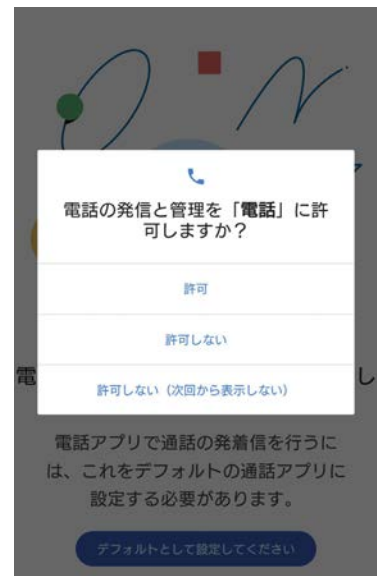
項目や文言は、使用する Android のバージョンやスマホメーカーによって異なりますが、アプリのインストール時に「不明なアプリ」と表示されたり、最初からオフに設定されている「不明なアプリ」に関する項目を変更させようとするものは、すべてセキュリティ上危険なものと判断するようにし、最初からオフの設定のままにしておくようにしましょう。アプリは、基本的に公式ストアからのみインストールするようにして、その他の場所からは避けましょう。

また、Android 機器でも iOS でも、アプリのインストール時や初回起動時に、同意を求められる「権限」▶用語集 P.196には充分注意してください。

権限とはインストールするアプリに対して、スマホのどの機能の利用を許可するか、という確認です。

単なるカメラアプリなのに住所録にアクセスするものや、撮影する必要がないのにカメラにアクセスするもの、著しく多くの項目にアクセスしようとするものなどは要注意の例です。項目別に許可を却下するか、そうできない場合、そのアプリは導入しないようにしましょう。また、最初は無害に見えて、導入後のアッ

### 導入時や起動時の権限付与に注意



#### ・Android、iOS (画面は Android)

アプリのインストール時や、起動時にさりげなく表示されるため、多くの人が無意識に「承認」や「同意」してしまっていますが、これは、「アプリがスマホのこれらの情報に自由にアクセスできる許可」を求めている画面です。

個別に却下することができない場合もあるので、その際は導入しないようにしましょう。そして、そもそも不必要な権限を求めるアプリは怪しいと警戒しましょう。

アップデートで権限の増加の許可を求めものも、その変更項目に注意してください。

その他、有用なアプリの開発者から、攻撃者が当該アプリを買い上げて、後からアプリをマルウェア化してしまう攻撃もあります。

このような場合は、ニュースサイトでそのような事案が紹介されることも多いので、情報収集時に気にかけておくといよいでしょう。

その他、アプリ間での機能連携やウェブサービス間で連携して、間接的に権限を奪取するものもあるので「連携」という言葉にも充分注意してください。

## ⑤メールの添付ファイルや本文中のリンクに注意しよう

### 標的型メールとスパムメールの例

#### 標的型メールの例



#### スパムメールの例 SMS(ショートメッセージ)を使った例



前節で述べた「偽メール」と類似しますが、添付ファイルやリンクは、標的型攻撃でもよく使われますし、今でもときどき復活しては、猛威を振るう「Emotet」も、マルウェアを添付したメールを受信者が開き、添付ファイルを実行することで感染が成立します。

心当たりのない送信元からのメールに添付されているファイルやリンクは、基本信用ならないものとして、むやみやたらに開かないようにするとともに、機器の設定などを堅牢に保ち、感染の隙を作らないようにしましょう。

スパムメールでの攻撃は、引っかけ率が少なくとも、その攻撃の母数を大きく取ることで攻撃者にとっての利益回収のパフォーマンスを上げています。

例えば、「フィッシングメールの例」の画面は、実際にSMSに送り付けられた、銀行を名乗るフィッシングメール▶用語集P.201を模したものです。

送信元とされる金融機関の口座を持っていない人であれば、フィッシング(=詐欺)メールだと気付くことができるかもしれませんが、現在もこういった攻撃に引っかかる人が一定の割合でいます。その先が詐欺サイトではなく、ゼロデイ攻撃▶用語集P.198のマルウェアが埋め込まれたウェブサイトならば、開いただけで感染してしまうでしょう。

また、もっとやっかいなのが、攻撃者ではなく、善意でマルウェアを拡散▶用語集P.195させてしまう人々です。友人から「このアプリ面白いよ!」と薦められたら、多くの人はあまり不審に思わないでしょう。

しかし、友人は知らなくても、実はこのアプリがマルウェア入りだったり、あるいは拡散する間は無害でも、後に権限を拡大して個人情報を抜き取るかもしれません。

これが、他人の発信ならば警戒できますが、親しい友達や家族だった場合、警戒するでしょうか?

対抗策としては、こういったお薦

め系のものは1つの線引きを持って接するようにしましょう。メールの文面など、目の前に見ている情報で完結しないものは一律に警戒するのです。動画が面白いとかお金が儲かる方法があるとかだけでなく、リンクでジャンプするとか、添付ファイルを開かせるものは一律に避ける。

それは、現実世界で「ちょっと向こうまで付き合ってよ」とか「ちょっとこの車に乗ってよ」といって連れて行かれるのに等しいと思ひましょう。

さらに、「リンクでジャンプしないけど検索エンジンで調べて見る分にはいいよね」、と思っても、攻撃者はそうやって検索エンジンからやってくる人向けに、二段構えでマルウェアを仕込んだウェブサイトを用意していることもある、と覚えておいてください。

## ⑥スマホやPCの画面ロックを利用しよう

### 7.1 スマホやパソコンには必ず画面ロックをかけよう

スマホやパソコン(PC)の情報を  
守る第一歩は、待ち受け画面にロ  
ックをかけることです。

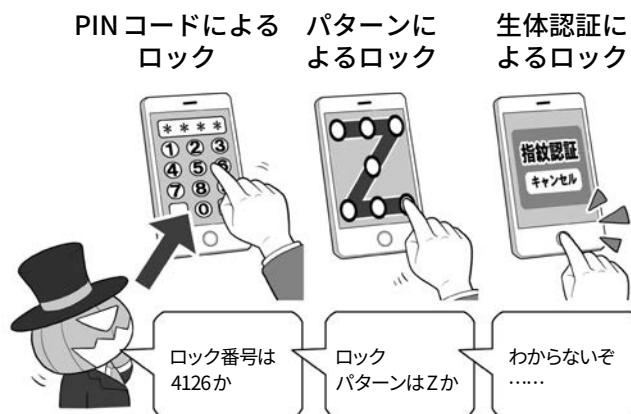
ロックには「PINコード\*」による  
ロック、パターンロック▶用語集 P.201、  
指紋や顔など生体情報を用いた認証  
によるロックなどがあります。ロッ  
ク機能は「誰かにスマホを持ち去ら  
れるなど、手元からスマホが離れた  
とき」に情報を確実に守るためのし  
くみの1つです。

とくに生体認証は周りから覗かれ  
PINコードを盗まれる危険性の排除  
をしつつ、入力の手間を省く  
ので便利な機能です。

指紋認証や顔認証が代表的ですが、  
その他にも、スマートウォッチ▶用語  
集 P.197 など特定のウェアラブル機器  
を着けたり、GPS▶用語集 P.191 に連動  
して自宅など特定の場所にいたりす  
ることで自動的にロックを解除でき  
るものもあります。

ただし、気を付けておきたいのは、  
セキュリティ向上のためのロック機  
能を設定しても、そのパソコンやス  
マホをロック解除したまま置いてそ  
の場所を離れたり、ロックを解除し  
て他人に見せたり貸したりすれば、  
一瞬で情報を盗み、乗っ取ることが  
可能です。画面ロックは、情報を保  
護するための強力なツールですが、  
ロック解除するための認証方法が脆  
弱だと意味がなくなります。ロック  
がかかっているから安心とそれだけ  
に頼り切りにならず、ロックを解除

#### スマホやパソコンにはロックをかけよう



#### 席において離れたり、人に貸したりしないようにしましょう



スマホを席に置いたままでは、本体も  
情報も盗まれるおそれがあります（とく  
にロックを設定しなかったり、ロック解  
除したままの状態で放置）。

スマホを貸すと、プライバシーを覗か  
れたり、一瞬でスパイ▶用語集 P.197 アプ  
リのようなものをインストールされたり  
することがあります。むやみに渡しては  
いけません。

するための機能や、スマホやパソ  
コンの管理にも留意しましょう。

スマホやパソコンは自分のすべて  
の情報が詰まった持ち歩く金庫だと

思って、必ず肌身離さず自分のそば  
に置き、使わないときはこまめにロッ  
クをかけた状態にすることが重要で  
す。

\* PINコードに関しても、詳しくはP.110以降のパスワードに関する項目を参照



## 7.2 よくある情報の漏れ方と対策

SNS用のアプリなどでは、本体のPINコードなどとは別に、アプリ専用のPINコードが設定できるものもあります。盗難などの際、SNSの内容を見られたくなければ、このアプリPINコードも設定しましょう。情報の守りが二重になります。一部の機種では生体認証をアプリのロック解除に利用できるものもあるので、セキュリティを向上させても快適な利用の妨げにはなりません。

一方、攻撃する側から見ると、スマホのロックをなんらかの方法でパスできたとしても、また、別の関門が待ち構えているわけで、手間をかけさせ侵入を諦めさせるというセオリーに沿っているわけです。

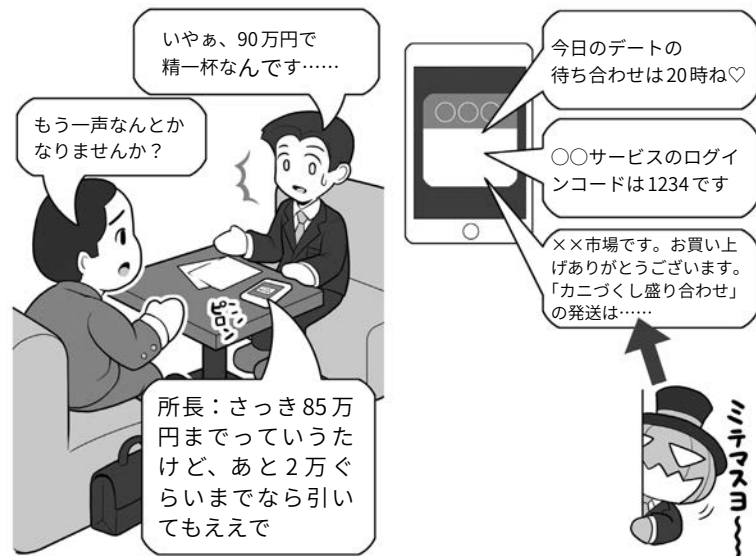
なお、アプリのPINコードを使う場合は、スマホロック解除のPINコードと異なるものを設定しましょう。PINコードの使い回しはセキュリティがないのと一緒にになってしまいます。PINコードもそれぞれ異なっこそ意味があるのです。

スマホをロックしていても情報漏れが発生することもあります。

例えば自分だけで使っているときは便利なメールの通知機能▶用語集 P.199。ロック画面▶用語集 P.204 にメールの内容を表示していると、誰かと会話中や商談中に、うっかり内部情報を見られてしまったり、あるいは差出人が分かるだけで、状況によっては知られると問題のある情報を提供してしまうことになりかねません。

また、同様にロック画面にメールの内容を表示していると、せっかくセキュリティ向上のために設定した多要素認証のパスワードメールも見られてしまうことがあります。そ

### 待ち受け画面に表示する通知はよく検討する



ロック画面だけでなく、普段使用している画面に通知ウインドウ▶用語集 P.199 として表示される場合でも、同じく情報を見られてしまう原因になります。スマホを使って説明しているときに、不適切なメールの内容が表示されることも……。情報漏えいには気を付けましょう。

### アプリごとにPINコードをかけられる場合はかける



本体のロックを解除されても、SNSのアプリに別のPINコードがあれば、流出の危険性は低くなります。それでも、自分が席を離れるときにスマホを残してはいけません。なお、勝手に他人のスマホのロック解除をすることは、れっきとしたサイバー攻撃です。

うするとスマホやメールアドレスの正当な持ち主であることを確認する役割を果たせず、画面を除き見た

けの第三者によって認証が突破できてしまいます。

# ⑦大切な情報は失う前に バックアップ(複製)しよう

## 8.1 何をするにもバックアップを取ろう

各種のサイバー攻撃や、パソコン・スマホの故障などからいち早く復旧して事業を継続するには、システムやデータのバックアップが不可欠です。とくに近年は感染するとファイルを暗号化して身代金を要求するランサムウェアの流行により、バックアップの重要性が格段に上がっています。バックアップの方法は主にパソコンやスマホのOSの種類により異なっています。パソコンの場合には、macOS搭載の機器のように、外付けの補助記憶装置▶用語集P.203(ハードディスクやSSD▶用語集P.192。以降記憶装置▶用語集P.195)を接続するだけでバックアップが行え、復旧もシステムとデータすべてをほぼ全自動で行えるものもあります。これに対してWindows搭載機器では、基本的にはデータをバックアップする考え方で、システムの復旧とデータの復元は、別に行うようになっています。

スマホの場合も機種ベンダーによる差もありますがほぼ同様です。

iOS搭載機器はパソコン上に専用の同期ソフトを導入して全体をバックアップします。この機能は機器を紛失した場合にも、新しい機器を接続すると全自動で復元が行えます。

Androidに関しては標準ではパソコンに全体をバックアップする機能はないので、Windowsに似た、データのみをバックアップする形で行います。なお、バックアップを取得す

### macOS 機器、Windows 機器のバックアップと復元

#### macOS



mac OS 機器はまるごとバックアップ、まるごと復元の性格が強く、Windows は基本的には OS を復元後、別途データを書き戻すイメージと考えるといいでしょう。

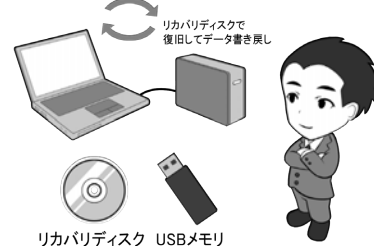
実際は他にも専用のソフトウェアを導入したり、細かい設定を変えることで、バックアップの方法を変える手段はあります。

ですから基本的なそれぞれの OS の立ち位置や性格と考えて下さい。善し悪しや優劣はありません。

#### Windows



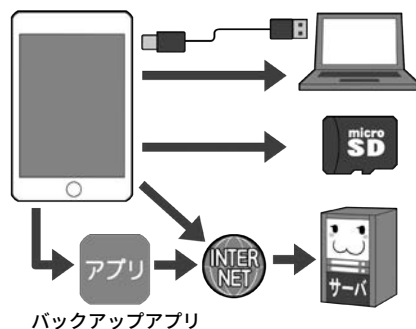
#### データをバックアップ



リカバリディスク USBメモリ

### スマホもバックアップは定期的にとろう

#### バックアップの方法はいろいろ



パソコンにつないで  
丸ごとバックアップ

内蔵できる microSD  
▶用語集 P.191  
メモリカードに  
バックアップ

直接あるいはアプリ  
経由でクラウドサーバに  
バックアップ

バックアップアプリ

#### なにがバックアップ できるか確かめる



なにがバックアップできるのか確かめて、機種やバックアップ方法を選択します。また、取得したバックアップを用いてシステムがちゃんと復元できるか確認してください。

るだけではなく、できれば取得した  
バックアップを用いてちゃんとシス

テムの復元を行えるか確認してくだ  
さい。

## 8.2 ランサムウェアや天災にも対応できるバックアップ体制

ランサムウェアなどの、データを破壊することが多いマルウェアの対策にはバックアップが有効ですが、では実際にどう運用するのでしょうか。

ランサムウェアはパソコンなどが感染すると、そのパソコンに繋がっている記憶装置すべてを暗号化してしまいます。仮にバックアップしていても、常時接続したままにしていると、その外付け記憶装置まで巻き添えて暗号化されることもあります。

そのため、バックアップ自体はマメにしておくべきですが、常時接続はしておかないという、かなり難しい運用が求められます。

また、最近は大雨による水害で、事務所にあったパソコンと外付け記憶装置が両方とも水没して復旧が困難になるという話もありました。これに対応する手段としては、バックアップの「3-2-1ルール」というものがあります。バックアップは本体を含め3個以上、2種類以上の媒体、そして1個は遠隔地に置くというものです。

遠隔地とは、現実的には「クラウドサーバ」▶用語集 P.195 などの利用を意味します。会社に同時に災害に遭わなような支社などがある場合は、そこにバックアップをおいてもよいでしょう。クラウドサーバは最近では手頃になりましたが、それでも本体の全データをバックアップできる容量は高価です。したがって、事業継続に必要な重要なデータを選別してバックアップすることになるでしょう。

なお、最近のクラウドでのバックアップはランサムウェアの巻き添えになりにくい規格のものもあるので、利用にあたっては調べてみましょう。

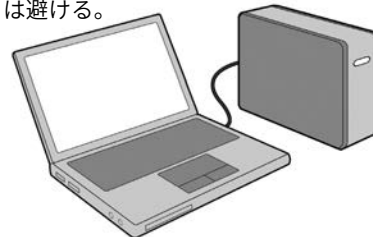
### ランサムウェア感染はビジネスにも影響



ランサムウェアはパソコン内のファイルを勝手に暗号化するため、感染すれば仕事上の極めて重要なファイルも人質に取られてしまいます。バックアップはまめにおきましょう。

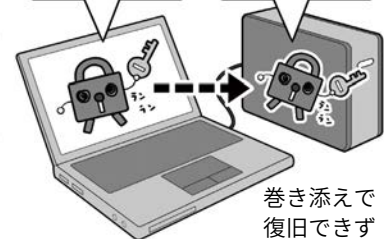
### バックアップの体制を整える

外付けバックアップ用記憶装置は可能な限り大容量のものを手配する。巻き添えにならないように常時接続は避ける。



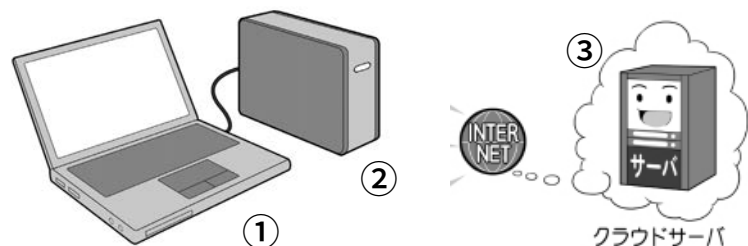
お、バックアップ用記憶装置発見! 暗号化しちゃえ

バックアップ用記憶装置暗号化完了



環境を整えたらバックアップを開始します。なにかソフトの導入や、環境を変更したらバックアップします。システムのアップデート後もバックアップします。ただし、バックアップ用記憶装置を常に接続しておくとなんらかの感染で巻き添えになって、復旧に使うためのデータも失われてしまいます。

### バックアップは3個以上、2種媒体以上、1個は遠い場所



本体+バックアップ用記憶装置+クラウドサーバで条件を満たします。クラウドサーバは多要素認証などで、攻撃者に乗っ取られないようにしましょう。



## ⑧外出先では紛失・盗難・覗き見に注意しよう

勤務先や外出先でスマホやパソコンを使う際に、誰かにスマホやパソコンを覗き見られている、そう感じたことはありませんか？

友人知人と冗談の範囲で「何やってるの〜？」と1回2回茶化すくらいならまだしもあまりに覗き見の頻度が高かったり、あるいは見知らぬ人に何も言わずにずっと横や後ろから覗き見られてたりしているようならば要注意です。

見られている内容が機密情報であったり、秘匿したい個人情報であったりする場合には、あなたの情報が漏れる心配があります。

「見られても大したことない情報しか自分のスマホやパソコンには保存してないよ」と心配しない人も多いかもしれませんが、覗き見している人はあなたの情報もさることながら、あなたがやりとりしている相手がターゲットかもしれません。

「ロックをかけてあるから大丈夫」と思っても、ロックを解除する方法がすでに相手の手に渡っている懸念もあります。例えば、相手に直接接触せず情報を入手する方法として、電車で座席に座っている人のスマホ操作を見てPINコードやパターンロック形状を盗む「ショルダーハッキング」、カフェなどのテーブルに放置されているスマホの画面に残る指の脂跡からパターンロックを見破る方法などがあります。P.40でも説明しましたが、飲食店などで席の確保にスマホなどを置き去りにする行為を時折見かけますが、紛失・盗難・覗き見、いずれの被害に遭って

### 外出時は自分のスマホやパソコンが他人から見られる可能性は高い



外出時は、使用しているスマホやパソコンを他人から覗き見されないよう注意が必要です。また、うっかり紛失して盗難されれば、大事な情報が盗まれるリスクは大きく高まるので、よく注意しましょう。

### スマホ使用時によく狙われるソーシャルエンジニアリング

#### ショルダーハッキング



公共の場でロック解除をするときは、背後などから見られていないか気を付けましょう。

#### 画面についた脂の跡を見る



スマホを席に残しておいたり、席取りのためにテーブルに置いて離れたりしてはいけません。

もおかしくない非常に危険な行為です。ついやってしまう、という人は

すぐにやめてください。



## ⑨困ったときは1人で悩まず、まず相談しよう

自らサイバー攻撃に気付いたり、あるいは第三者からの連絡で気付いた場合は、直ちに処置を取り、その後必要な各種窓口で相談しましょう。

あらかじめ対応者を決めてあるならば、その人を中心に対応するか、決めていない場合には、ITに詳しい社員などがいたらその人を中心に対処しましょう。

一番最初にするべきは電源を落とさないままインターネットから切断することです。これはマルウェアなどの拡散を防ぎつつ、後々警察に連絡をする場合の証拠保全になります。

次に、連絡するには状況を把握しなければならないので、なるべく分かる範囲で5W1Hのように分けて事象を記録しましょう。いつから始まったのか、どのようなことがあったのか、誰が作業していたのかなどです。当然のことながらその間、攻撃が行われたと思われるパソコンなどの機器は使わず、その他の機器や紙のメモで記録します。

サイバー攻撃を受けたときに相談するサービスを契約している場合はそちらに相談し、無い場合は、IPAの「情報セキュリティ安心相談窓口」のウェブサイトを検索して、類似の例がないか調べてから、電話やメールで相談しましょう。

ランサムウェアによりデータを暗号化されて脅迫されたり、情報を消されたり、何か機器を故障させられたり、あるいは情報を盗難されたりなど、明確に被害がある、もしくは被害に遭ったおそれがある場合は、各都道府県警のサイバー犯罪相談の

### 各種連絡窓口のウェブサイトなど

#### IPA「情報セキュリティ安心相談窓口」

<https://www.ipa.go.jp/security/anshin/>  
電話番号：03-5978-7509(平日 10:00-12:00, 13:30-17:00)  
メールアドレス：anshin@ipa.go.jp

#### IPA「J-CRAT/標的型サイバー攻撃特別相談窓口」

<https://www.ipa.go.jp/security/tokubetsu/index.html>  
メールアドレス：tokusou@ipa.co.jp

#### 東京中小企業サイバーセキュリティ支援ネットワーク (Tcyss)「中小企業サイバーセキュリティ相談窓口」

<https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/joho/tcyss.html>  
電話番号：03-5320-4773(平日 9:00-12:00, 13:00-17:00)

#### 都道府県警察「サイバー犯罪等に関する相談窓口」

<https://www.npa.go.jp/cyber/soudan.html>

#### 消費者庁「消費者ホットライン」188

[https://www.caa.go.jp/policies/policy/local\\_cooperation/local\\_consumer\\_administration/damage/](https://www.caa.go.jp/policies/policy/local_cooperation/local_consumer_administration/damage/)  
電話番号：188

#### 個人情報保護委員会「漏えい等の対応とお役立ち資料」

<https://www.ppc.go.jp/personalinfo/legal/leakAction/>

窓口などに相談しましょう。

そして自社や団体で扱っている個人情報を盗まれたり消されたりしてしまった場合、「望ましい対応」として、原因究明や再発防止策の策定、そして「努力義務」として個人情報保

護委員会などへの速やかな報告が求められます。

従来はファックスや郵送での報告ですが、令和元年3月からは、ウェブサイトからフォーム入力による方法で報告できるようになりました\*。

\* 詳しい報告先や対応方法は個人情報保護委員会ウェブサイトをご覧ください。

## コラム.1 攻撃されにくくするには、手間(コスト)がかかるようにする

サイバー攻撃を行う攻撃者は、軍事や産業スパイ、名をあげることで自体を目的に採算度外視でやる悪意のハッカーなどではない場合、なんらかの利益が目的の行動が多いといえることができるでしょう。

彼らにとってのサイバー攻撃はビジネスであり、ビジネスはコストパフォーマンス、つまりいかに手間をかけず大きな利益を生むかが重要です。

そういった攻撃者の視点から見ると、攻撃されにくい環境を作るにはどうしたらよいかが見えてきます。

例えば、現実世界では、泥棒は防犯がしっかりしていて警戒が厳重な家よりも、鍵をかけなかったり窓を開けっ放しで外出したりするような家の方に侵入します。その方が、彼らにとって安全、つまり手間(コスト)がかからないからです。

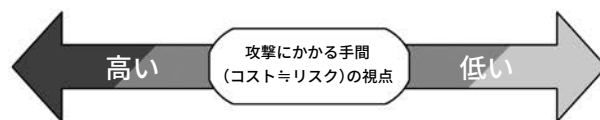
これは、ネットの世界でも同様です。侵入するまでに幾重にも難関があり、侵入を試みたら形跡を記録され(ログ▶用語集 P.204)、場合によってはしかるべき管理者に通知が行き、パスワードを破ろうとしても複雑で突破できない。システムも最新で、攻撃するにもセキュリティホールが見あたらない。セキュリティソフトも導入されている。さらに、ファイルを盗めても複雑な暗号化がされていれば、解読までに何百年もかかってしまい使えない。普通の攻撃者なら敬遠します。

横を見たら、セキュリティホールは放置、パスワードは非常に簡

### コスト 攻撃されにくくするには手間がかかるようにする



現実の世界



ネットの世界

単だったり無しかったり、ファイルそのものも暗号化されておらず、パスワードを使っていても、皆さんのウェブサービスで全部同じものを使い回している。

これならば、どっちに行くのがビジネスとしてコストパフォーマンス

ンスがよいか明らかですね。

こういった攻撃者の視点を持ち、侵入することがとても面倒くさく、攻撃したくなるような環境を構築するのが安全への近道です。一方、単純な利益目的でない場合、すこし対策が変わってきます。

## コラム.2 利益が目的ではない攻撃に備えるには

金銭などの利益目的ではない攻撃の例としては、相手そのもの、つまり未成年者略取や、いかがわしい写真の入手などを目的とするものがあります。

現実の世界で、面と向かって「いかがわしい写真を撮らせてください」といったら、たいていの人は拒否して逃げ出すでしょう。それが、ネットの世界だと許容してしまう理由は、攻撃者がネットを利用して、警戒心をもたれないような人間になりすまし▶用語集 P.200、相手をうまくだましてしまうからです。

ですから、SNSや掲示板などのウェブサービスで知らない人物が近付いてきたら、注意して絶対に個人情報は教えないようにしましょう。現実の知り合いでもないのに会おうと誘われた場合は、基本的に会わないか、会う必要がある場合は必ず保護者同伴で行きましょう。

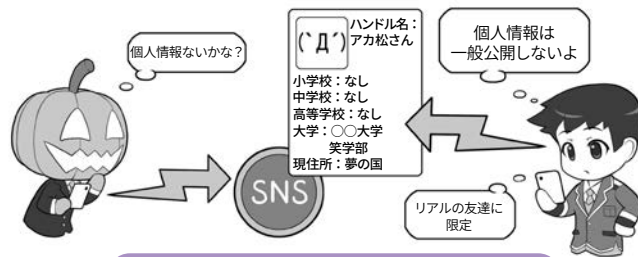
そして、少しでも変だなと思ったり、最初と話が違ったりした場合、それは人をだます「心理的な」テクニックかもしれません。警戒し、その場から立ち去りましょう。

あまり聞いたことがないかもしれませんが、そういった「人をだます心理的なテクニック(≡ソーシャルエンジニアリング▶用語集 P.198)」は体系化されマニュアルのようになって存在するのです。

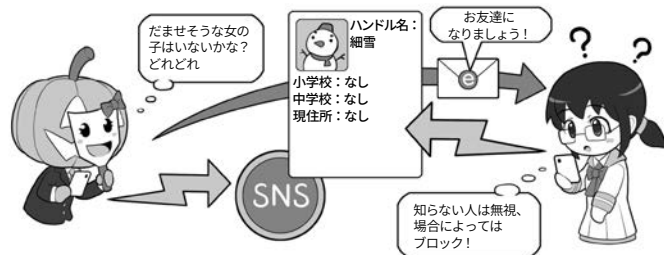
この人をだますテクニックは、なにも上記のような例だけでなく、私たちも日常生活のさまざまなシーンで直面しているのです。

例えば、「振り込め詐欺」や「標

### 金銭目的ではない攻撃にも備えよう



個人情報是一般公開にしない



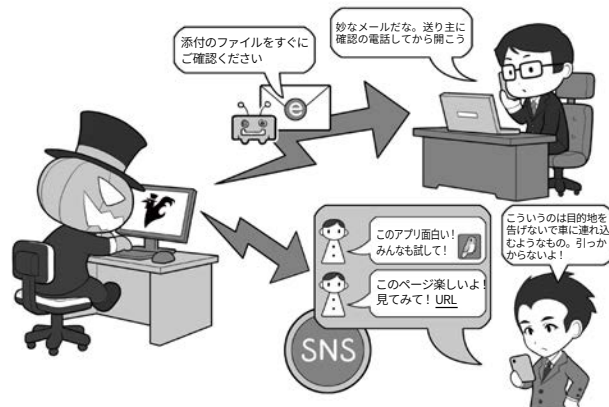
リアルで知り合いじゃない人とはネットで友達にならない！

未成年が SNS を利用する場合、写真や自分の個人情報を記載しないようにしましょう。また、投稿内容も原則的に一般に公開せず、SNS で友達になった人のみが見られる設定にしましょう。

SNS で、知らない人が友達になるとリクエストを送ってきても、会ったことがない人はスルーするか基本的にお断り（ブロック）しましょう。

それは、現実の世界で自分の個人情報を書いた名札を付けて歩いたり、名前もわからない初めて会った人に、ついていったりするのと同じぐらい、たいへん危ないことなのです。

### 攻撃者に操られて、内側から鍵を開けてしまわないように、心がまえを持とう



不審なメールに気を付け、怪しいときは開かず送信者に確認する癖を付けましょう。ネットや SNS の引っかけは、セキュリティ関係のニュースをこまめに見ていると、次第に傾向がわかるようになります。訓練しましょう。

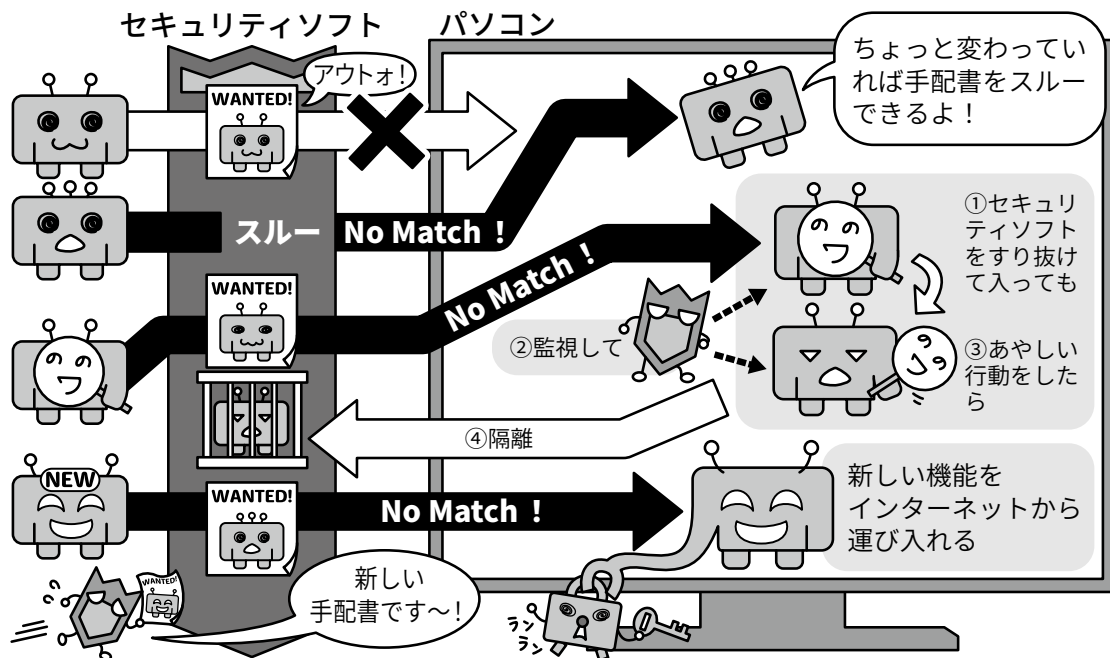
的型メール」。どんなにセキュリティを固めても、本人がだまされ結果として犯罪者に操られてしま

うと、すべては無意味になってしまいます。厳重に注意しましょう。



### コラム.3 セキュリティソフトを導入しても過信しないことが重要

どんなセキュリティソフトでも、既知のマルウェア対策には有効だが、存在を知られていない新たな攻撃への対策は難しい



最近、一部のSNSやブログでは、「セキュリティソフトは不要」という論調の記事を見かけることがあります。本当に不要でしょうか？

個人利用の範囲では、OS標準で付属しているセキュリティソフトで事足りることも多く、企業利用でもOS標準のセキュリティソフトを用いることが増えています。

しかし、業務で使う場合、単純に攻撃をどれだけ防いでくれるか？という指標以外にも、複数のプラットフォームへの対応状況、企業内の端末管理用機能などもセキュリティソフト選びにおいては重要になってきます。

また市場流通するセキュリティソフトでは、パスワードマネージャーやネットバンキング保護など、OS標準のソフトには備わっ

ていない機能も多く、ユーザーのさまざまな利用シーンに配慮している特長があります。

ただ、OS標準版、市場流通版、いずれにしる使用する際留意すべき点として共通しているのは、セキュリティソフトをパソコンやスマホにインストールした後は、アップデートし最新の状態を保つことです。なぜアップデートが重要かというと、セキュリティソフトがマルウェアを見つける方法に理由があります。

マルウェアを見つける方法は、事前に登録したマルウェアと同じ挙動をするプログラムを駆除する「手配書」方式、パソコン内に侵入された後も監視を続け不審な挙動があれば隔離や駆除を行う「ふるまい検知」、機能的に怪しい部分

を検出する「ヒューリスティック分析」▶用語集P.201 機能などが挙げられます。

これらは既知のマルウェア、既知の悪意あるふるまいを行うプログラムへの対策には有効ですが、検体▶用語集P.196 が十分に収集されていないマルウェアや、まだ存在を知られていない全く新しいマルウェア、新たに考案された悪意あるふるまいの検知は難しいとされています。

セキュリティソフトを導入しているからといって過信はせず、「あやしいリンクはクリックしない」「見覚えのないメールは開かない」と本ハンドブックでも解説する基本的なセキュリティ対策の徹底が重要です。



## 第2章

# よくあるサイバー攻撃の 手口やリスクを知ろう

基礎的なセキュリティを固めても、インターネットにつながる限りサイバー攻撃を受けてしまうリスクはあります。実際にサイバー攻撃を受けてしまうとどんな被害があるのでしょうか。乗っ取りやランサムウェアなど、よくある被害について学びましょう。

### 1 攻撃者に乗っ取られると起こることを知ろう

- 1.1 被害に遭わないために。そして加害者の立場にならないために
- 1.2 盗まれた情報は犯罪に使われる
- 1.3 乗っ取られた機器はサイバー攻撃に使われる
- 1.4 IoT 機器も乗っ取られる。知らずにマルウェアの拡散も…

### 2 大きな脅威となっているランサムウェアを知ろう

### 3 フェイクニュース、サイバープロパガンダに騙されないようにしよう

**コラム1** それでも間に合わないゼロデイ攻撃

## 1

# 攻撃者に乗っ取られると 起こることを知ろう

## 1.1 被害に遭わないために。そして加害者の立場にならないために

攻撃者▶用語集 P.196 があなたのパソコンなどにサイバー攻撃▶用語集 P.196 をしかけるのは、お金や情報を盗むだけでなく、あなたのパソコンなどをサイバー攻撃の道具にする目的である場合もあります。

手順としては、あなたのパソコンなどをマルウェア▶用語集 P.203 に感染させるか、流出したID▶用語集 P.191 とパスワード▶用語集 P.200 を使いパソコンに侵入し、自由にコントロールできるようにします。

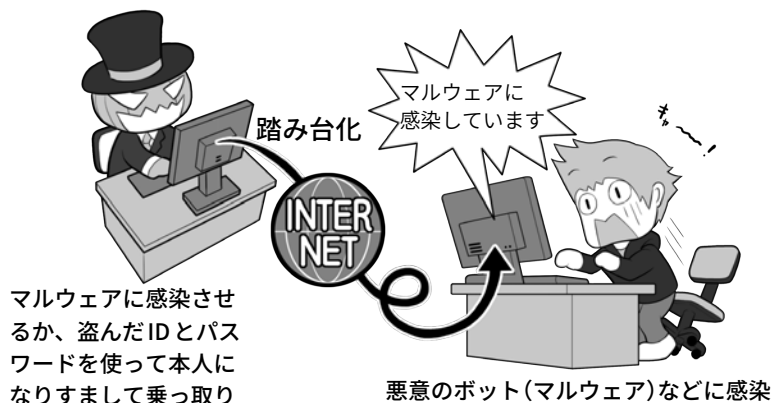
次に別のパソコンやサーバなどに侵入するとき、「踏み台▶用語集 P.202」にしてあなたのパソコンがやっていると見せかけたり、悪意のボット▶用語集 P.203 によるボットネット▶用語集 P.203 に接続させ、第三者へのDDoS 攻撃▶用語集 P.190 を行わせたりします。

こうすることで、万が一サイバー攻撃がばれたとしても、最初にあなたが調べられ、その間に攻撃者は証拠隠滅などをして姿をくらますことができるわけです。

こういった場合でも、入念に調査すれば乗っ取られていた事実が分かるでしょうが、もし攻撃が重要な社会インフラに対して行われ、実際に被害者が出てしまったら、あなたは思い悩んでしまうでしょう。

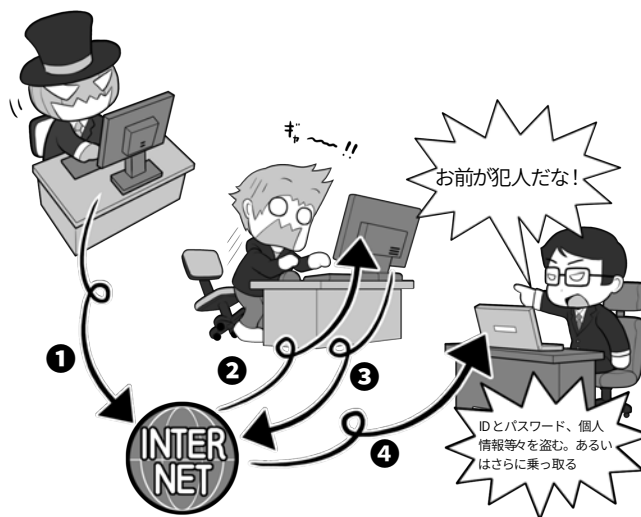
そうならないためにも、公衆衛生的なマナー意識を持って、パソコンなどのセキュリティはしっかり固めましょう。もしセキュリティソフト

### 攻撃者によるパソコンなどの乗っ取り



攻撃者は、目的のパソコンなどをマルウェアに感染させ乗っ取る他、流出したあなたのIDやパスワードを利用してあなたになりすまし、各種サービスやリモートでパソコンにログイン▶用語集 P.204 を試みて、これに乗っ取ります。マルウェアであればセキュリティソフトで検出されるかもしれませんが、なんらかの正規の方法でログインされ、「本人」としてリモートコントロール用のソフトをインストールされると、その乗っ取りに気付くのは困難になります。

### 乗っ取ったパソコンを踏み台にしてサイバー攻撃を行う



攻撃者は乗っ取ったパソコンなどに対して①インターネットを通じて、②乗っ取ったパソコンに指示を出し、③あなたのパソコンがやっているように見せかけて（踏み台化）、④他の人のパソコンに攻撃をしかけます。攻撃者はこうすることで自分の存在を隠して、安全にサイバー攻撃を行えるわけです。

また、乗っ取りだけでなく、あなたのパソコンのメールアドレスを使って、他者にフィッシング詐欺のためのBEC（ビジネスメール詐欺）▶用語集 P.190 のメールなどを送信する場合もあります。

▶用語集 P.198 が、マルウェアに感染していることを検出したら速やかにネットから切断し、実害の出ている

攻撃に関して、警察などから協力の要請があった場合は証拠保全 (P.106 参照) を行いましょう。

## 1.2 盗まれた情報は犯罪に使われる

攻撃者は、あなたのパソコンなどを乗っ取って、個人情報▶用語集 P.196、クレジットカードや銀行情報、ウェブサービスやSNS▶用語集 P.192 のIDとパスワードなどを盗むと、それを犯罪に使います。

例えば銀行のインターネットバンキング▶用語集 P.194 を使った不正送金▶用語集 P.202 で、口座からお金を盗み取るかもしれません。

銀行のインターネットバンキングは多要素認証▶用語集 P.198 でガードがされているから大丈夫と思っても抜け道はありますし、あなたの情報を売ってお金を得る手段もあります。

流出したクレジットカードを使いオンラインで勝手に買い物をして、それを受け取り現金化する、といった事件も起きています。

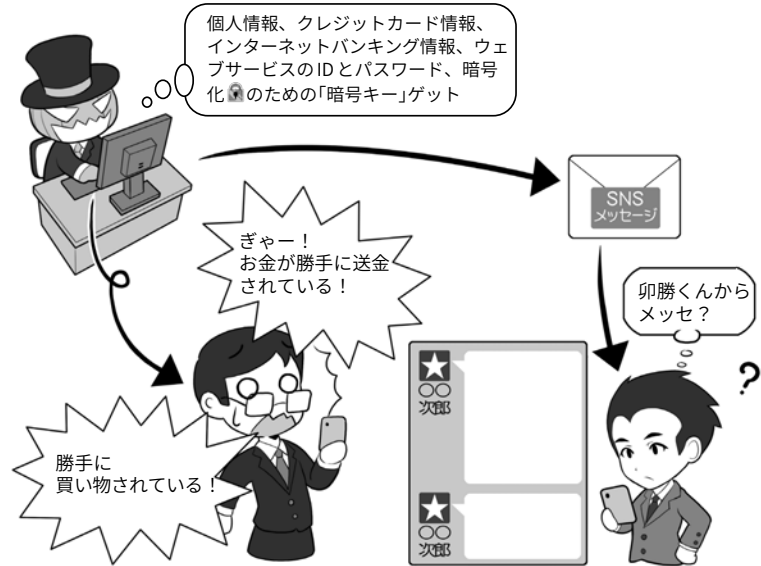
SNSのメッセージであなたになりすまし▶用語集 P.200、友だちに対して「プリペイドカードを買って、アクティベーションコード▶用語集 P.194 を送ってくれ」と依頼して、電子マネーをだまし取る場合もあります。

自分が使っているパソコンなどのセキュリティをしっかり固めていても、情報を登録しているウェブサービスなどから、間接的に流出・盗難されることもあります。

この場合でも同じように、攻撃者は盗んだ情報からなんらかの手段を用いて、お金を手に入れようとします。あなたに非がなくても流出は起こるのです。自分の環境のセキュリティを固めてもそのときは防ぎようがないので、不正利用などの兆候に気を付けてください。

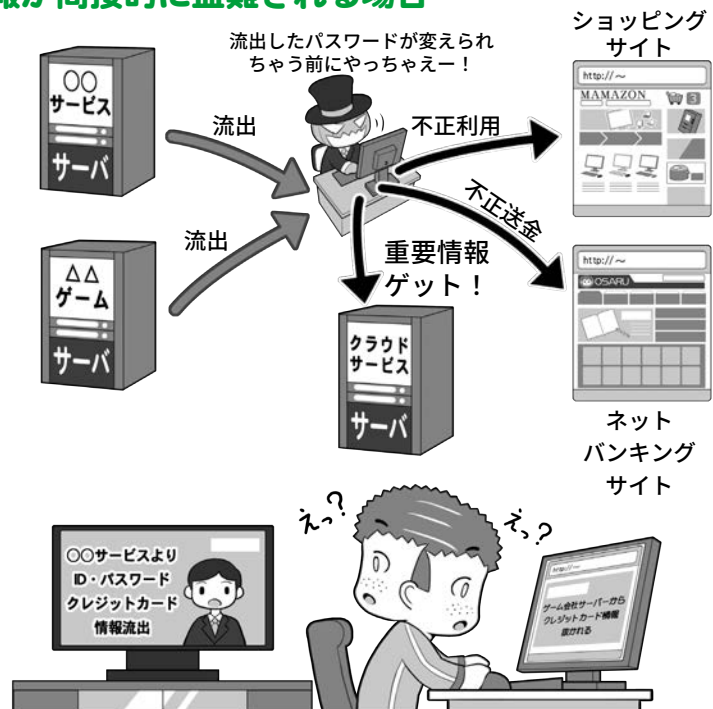
パスワード流出が判明したらパスワード設定のセオリー(P.32,P.110)

### 情報が直接盗難される場合



クレジットカード情報の流出などが起こった場合は、その被害は多岐に及びます。とりえずカードが不正利用されていないかチェックしましょう。パスワードなどの流出が判明したら、該当するサービスのパスワードの変更を行いましょう。

### 情報が間接的に盗難される場合



特定のサービスからIDやパスワードが流出しただけならば、IDとパスワードの使い回し▶用語集 P.201 をしていない限り、他のサービスへの被害拡大はありません。しかし、使い回しをしている場合や、クレジットカード情報が漏れた場合、その被害は多岐にわたる可能性があります。楽観的に考えずに迅速に対処しましょう。

にしたがってすぐに変更し、クレジットカード情報が流出したらカード会

社に連絡してカードの番号を変更しましょう。

## 1.3 乗っ取られた機器はサイバー攻撃に使われる

サイバー攻撃で攻撃者に乗っ取られたパソコンなどの機器は、「ゾンビ化」といい、攻撃者に操られる状態となって、さまざまなサイバー攻撃に使われることがあります。

サイバー攻撃の「踏み台(身がわり)」に使われる他、「悪意のボット」に感染した機器は、持ち主の知らないところでボットネットというゾンビ化したIT機器の集合体に加えられ、攻撃者の命令で特定のサーバに一齐にアクセス要求をするDDoS攻撃などに使われます。

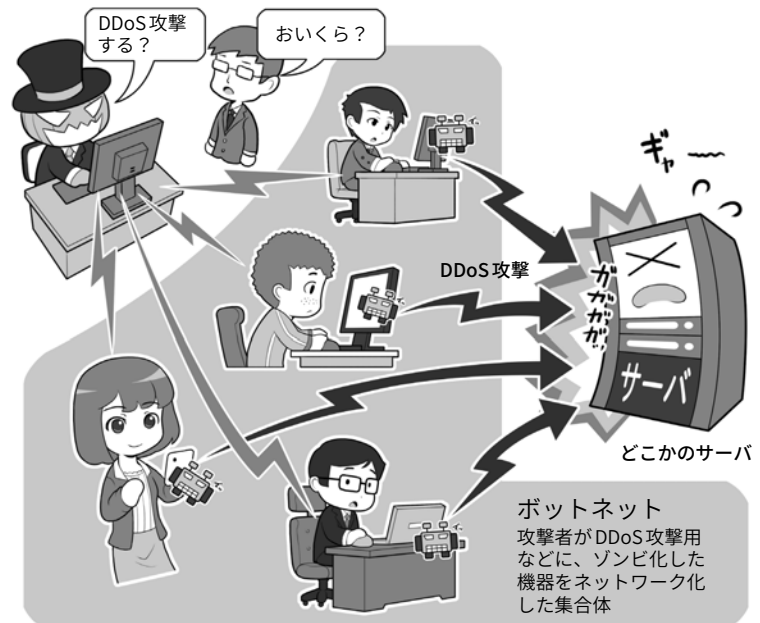
このボットネットによる攻撃は、攻撃者が自分の技術や主張を誇示する行動などにも使われますが、ボットネットを利用して攻撃を行いたい人物に、時間あたりいくらで貸し出されたりもします。攻撃者は乗っ取った人の財産(パソコンなど)を勝手に貸し出し、違法にお金を稼いでいるわけです。

一方、「踏み台」的な攻撃はパソコンなどの乗っ取りによるものだけではありません。

「ウォードライビング」とって、車に乗って、会社や事務所に設置されている、暗号化されていない、もしくは暗号化▶用語集 P.194 や暗号キー▶用語集 P.194 の設定の甘い無線LANアクセスポイント▶用語集 P.203 を探し、見つけるとこれに侵入して利用する手法があります。

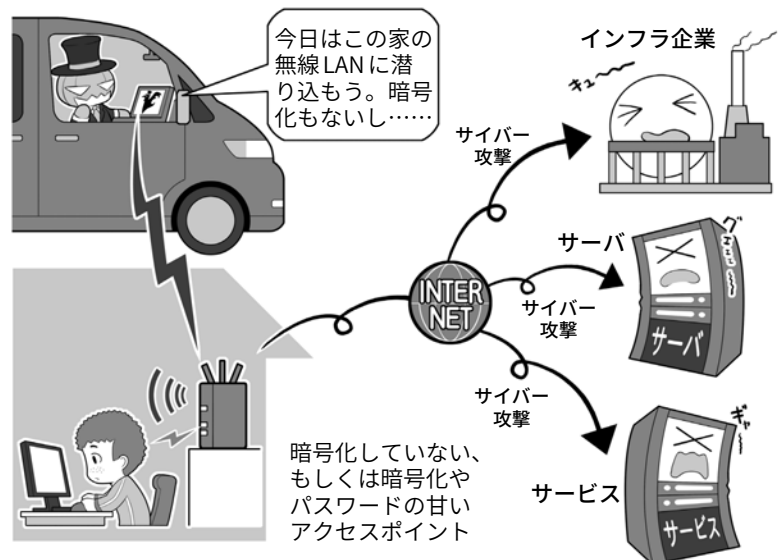
これはアクセスポイント▶用語集 P.193 を「踏み台」にし、そこからインターネット上のさまざまなサーバやインフラ企業に攻撃をしかけるためです。攻撃をしかけてきているのは「踏み台」がある場所と見せかけて身代わりにし、攻撃がばれたときの追跡を

### 乗っ取られたマシンはボットネットとして貸し出される



攻撃者によって悪意のボットに感染させられ、コントロールされたパソコン(ゾンビPC)などの集合体がボットネットです。攻撃者の命令で、一齐に特定のサーバなどにDDoS攻撃をしかけ、ダウンさせたり反応不能に陥れたりします。ダークウェブ▶用語集 P.198などで時間あたりいくらという形で貸し出されることもあります。

### 無線LANに侵入され罪を押し付けられることも



車で街を徘徊して、侵入可能な無線LANアクセスポイントを探すことを「ウォードライビング」といいます。こういった侵入を許し「踏み台」にされないためには、無線LANアクセスポイントのセキュリティ設定をきちんと見直しましょう。それが、自分の身の回りのできるサイバー攻撃阻止の第一歩です。

逃れるためです。

この場合、攻撃者に非があるのが当然ですが、会社や事務所からサイバー攻撃が行われ、インフラ企業な

どで事故が発生したら心中穏やかではありません。セキュリティを固めて侵入されないようにしましょう。



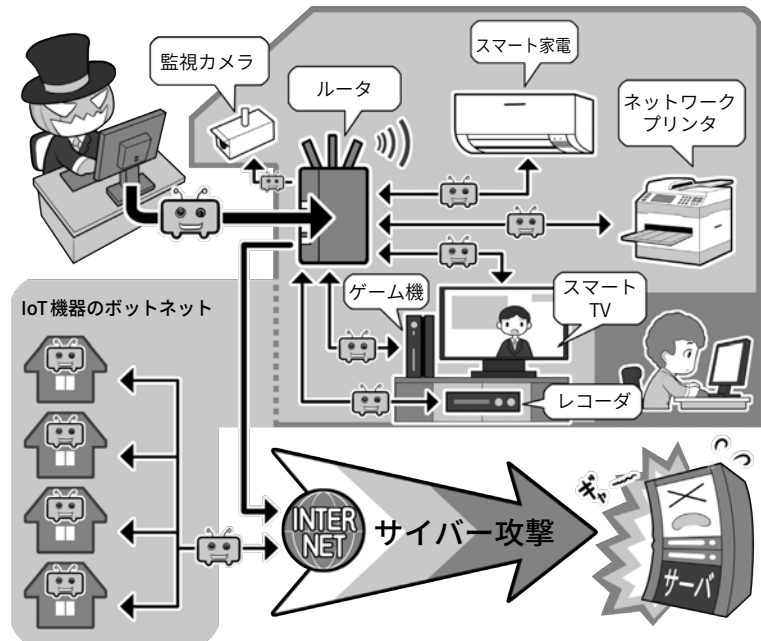
## 1.4 IoT機器も乗っ取られる。知らずにマルウェアの拡散も…

攻撃者によって乗っ取られるのはパソコンやスマホだけではなく、ネットにつながるIT機器はいずれも、乗っ取られて攻撃者の身代わりにされる「踏み台」化、DDoS攻撃のボットネットへの接続、マルウェアの拡散▶用語集 P.195 など、さまざまなサイバー攻撃に利用される可能性があります。とくにIoT機器は、監視カメラやネット対応電子機器などのように、普段私たちがあまりセキュリティについて気かけないものであり、パソコンほどサイバー攻撃への対応能力も高くありません。そして1つの機種で生産台数が多い＝手間をかけずに多数を一気に攻撃できる「攻撃しやすい条件」が揃っているのです。最低でも、IoT機器の出荷時の「管理者用パスワード▶用語集 P.195」などはパスワードセオリー(P.32,P.110)にしたがって変更し、システムは最新に保ち、ネットにつながりが必要ないものはむやみに接続しないようにしましょう。

また、サイバー攻撃に協力してしまうのはなにもパソコンやIoT機器だけとは限りません。人間は最大のセキュリティホール▶用語集 P.198 ともいわれ、マルウェアの拡散源となることもあります。SNSなどで「この記事が面白いよ」「このアプリ▶用語集 P.194 試してみて」といった投稿を考えなしに拡散していると、その先はフィッシングサイトだったり、マルウェアのようなアプリだったりということもあり得ます。

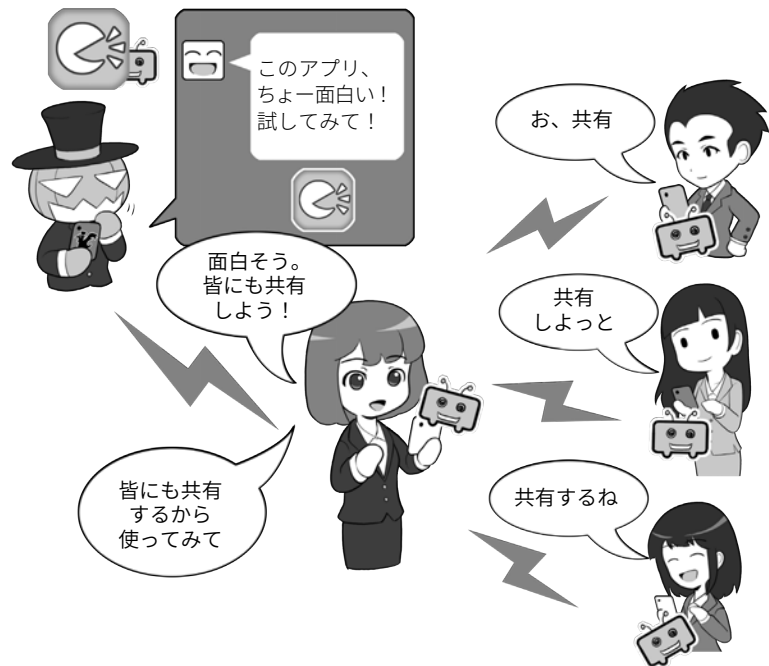
ネットでなにか行動する前には、必ず「それは本当に必要なのか」「そうすることでなにか問題が発生する可能性はないのか」をいつも注意しましょう。

### IoT機器も乗っ取られ攻撃に使われる



IoT機器は攻撃者から見ると、乗っ取りやすい要素を多く持っています。攻撃者はそれらを乗っ取ってさまざまなサイバー攻撃に使います。IoT機器は最低でも「出荷時の管理者パスワードの変更」「システムの状態を最新にする」「必要のない機器はネットにつながらない」などの対応をしましょう。

### 知らずにマルウェアの拡散に協力しているかも……



SNSで見た「面白い投稿」や「拡散希望の投稿」を深く考えないで拡散すると、その投稿にあるリンクの先にはフィッシングサイト用意されていたり、ゼロデイ攻撃▶用語集 P.198 のマルウェアが仕込まれていたり、アプリであればマルウェアが入ったものだったり、そのときは違っても、のちのちそう変化するアプリかもしれません。拡散する前によく考えて「共有する必要がないものは共有をしない」ようにしましょう。そうしないと、あなたが被害者ではなく、サイバー攻撃やマルウェアの拡散者になってしまうかもしれないからです。

# 大きな脅威となっている ランサムウェアを知ろう

パソコンなどのデータを暗号化し開けないようにして、身代金を要求するランサムウェア▶用語集 P.203。その大規模な感染に注目が集まっています。

例えば、2021年10月には、四国の病院で稼働しているシステムにランサムウェアが感染し、病院の診療を停止せざるを得なくなった上、復旧に2ヶ月以上を要するという事態になりました。また、この数年ランサムウェアによる国内被害の報告件数は増加し続けており、2020年下半期が20件だったのに対し、2022年上半期のランサムウェア被害は114件と6倍近い数になっています。なお、これはあくまで「報告された件数」であり、報告されない被害も相当数あると考えるのが妥当です。

近年では感染経路が多様化しており、メールを経由して不審なファイルをインストール▶用語集 P.194 させられるだけでなく、脆弱性の存在しているVPN▶用語集 P.193 機器を経由して外部から侵入されるケースも見受けられます。

また、脅迫の手法についても、暗号化したデータの復号▶用語集 P.202 をもちかけて身代金を要求することに加え、盗んだデータを外部に公開するという脅しをかけ、さらなる身代金を要求するケースも出てきています。

日本の大手企業がこのような新たな経路や手法により、被害を被った事例もありました。

こういったランサムウェアでは、身代金を支払ってもデータの暗号化

## ランサムウェア感染はビジネスにも影響



ランサムウェアは、パソコン内のファイルを勝手に暗号化するため、感染すれば仕事などをする上で極めて重要なファイルも人質に取られてしまいます。バックアップは常に行っておきましょう。

## ランサムウェアの被害を受けたら悩まずすぐに相談！

ランサムウェアによる攻撃や情報の無断公開はれっきとした犯罪です。被害を受けた場合は、警察への通報・相談などをしましょう。NISC▶用語集 P.191 としてもランサムウェア対策のための対応手順や情報を公開しています。

警察庁 サイバー犯罪対策「ランサムウェア被害防止対策」  
<https://www.npa.go.jp/cyber/ransom/>  
 NISC「ストップ！ランサムウェア ランサムウェア特設ページ」  
<https://security-portal.nisc.go.jp/stopransomware/>

を解除できなかったり、外部公開されたりするケース也多発しており、最悪の場合は端末を初期化▶用語集 P.197 しなければならず、大切なデータが失われることにもなりかねません。

ランサムウェアに感染してこういった事態に陥らないよう、システムやアプリは最新の状態に保つ、データを常にバックアップ▶用語集 P.201 する、必要に応じてセキュリティソフトを利用するなどの対策をしっかり実施しましょう。また、不審なメールのリンク▶用語集 P.204 をクリックしない、あやしいウェブサイト▶用語集 P.194 からソフトやアプリをインストールしないよう意識することも重

要です。ただ、最も大事ななのは、企業や団体が、組織としての方針を示した上で、前述のような対策を徹底することです。

まずは「事前」に、ランサムウェアも含め、マルウェアに感染した場合の対応ポリシーや手順を策定するとともに、感染した場合には策定したポリシーや手順に則った対応をしてください。

なお、ランサムウェアによる攻撃や情報の無断公開は犯罪なので、対応手順などは、警察への通報・相談なども視野に入れましょう。

# フェイクニュース、サイバープロパガンダに騙されないようにしましょう

悪意を持った者が、なんらかの意図を持って、ネット上で偽のニュースを発信する「フェイクニュース」▶用語集 P.201」。SNSなどで拡散され始めるとニュースサイトなどでも真贋不明のまま取り上げられ、それを真実だと思う人が多数現れてしまうということが起きています。

フェイクニュースには、意図を持って発信している人の他に、人々が注目するニュースをねつ造することで自分のウェブサイトの閲覧数を増やし、掲載した広告の収入でお金を稼ぐ商売としている人もいて、1つの悪意のビジネスモデルになっています。

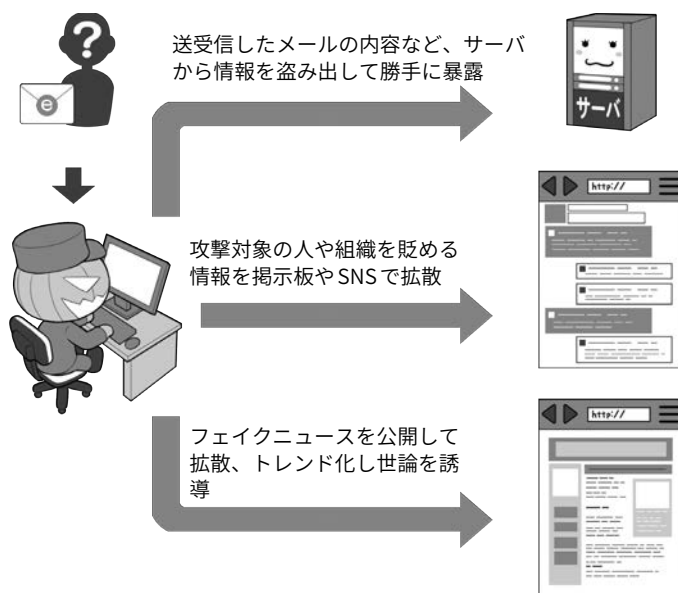
検索エンジン企業やSNS企業などは、こういった情報がニュースのランキングに登場しないように工夫をしたり、善意の団体と協力して偽の情報の場合は否定するなど処置を行ったりしていますが、いまだ根本的な解決には至っていません。

こういったフェイクニュースを、外国の国家機関が「武器」として使い、他国の選挙における投票行動などに意図的に影響を及ぼす「サイバープロパガンダ」▶用語集 P.196 も多く発生しています。

プロパガンダ自体は、古くから国家が自国や他国に対して影響を及ぼすために、行われてきた「人を思いどおりに動かそうとする情報の悪用法」ですが、これがネットを使うことで高度化かつ秘密裏になり、人々が気付かぬ間に、その考え方が操作される事態が起きているのです。

これを行うため、サイバー攻撃に

## サイバープロパガンダが行われた例(米国)



サイバープロパガンダでは、フェイクニュースや盗んだ情報のリークを種として、トロールと呼ばれる情報操作グループと「いいね」や「共有」を押す自動のボットによりこれをトレンドにのせ、さらに、ターゲットの国の「自分にマッチした情報を好んで共有する」人たちのSNS 集団（エコーチャンバー）にこれを投げ込み、最終的にその他大勢に、さも「重要なニュースである」というイメージを与え、世論を操作します。

よって盗んだ政治家のメールを改ざんした上での暴露、国と密接な関係にあるメディアでの偽ニュースの発信、ボットを使ったSNSでの偽ニュースのトレンド化、政治的な争点になっている事柄の賛否両方にSNS上で広告を打つことで混乱を生み出し国民を分断、そして、SNS上で架空の人格のアカウントを作りインフルエンサー(有名人)に成長させ、他国の人々を自国に有利になるように扇動するなどといった、さまざまな手法を総動員してサイバープロパガンダが行われているのです。

私たちが希望を持つインターネットでは、一方でそういった悪意を持った人々が暗躍しているということを

理解し、フェイクニュースやサイバープロパガンダ発の情報への対抗には、情報の受け手が「疑わしいときは一次情報を調べる」「他の情報と比べてみる」「情報の発信元を確かめる」などの基本行動を取る、もしそれが「無理」となったら、身近にいる信頼できる人に聞いてみたり、それすら難しい場合には「一旦情報から距離を置いて、冷静になって考える」などの方法が有効です。

なぜなら、サイバープロパガンダには、私たちが「深く考えず情報を拡散する習性」までもが組み込まれているからです。悪意のある人の駒にならないように気を付けましょう。



## コラム.1 最新の状態に保っても間に合わないゼロデイ攻撃

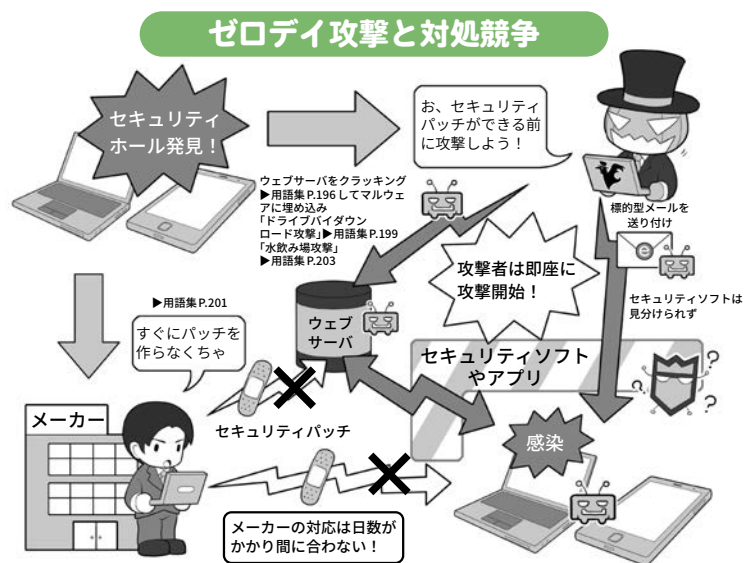
一般的にはシステムやソフトにセキュリティホールが見つかったら、攻撃者はこの穴を攻撃するためのマルウェアを急いで開発し始めます。メーカーもこの穴に気付けば、アップデート▶用語集 P.194 用のセキュリティパッチ▶用語集 P.198 を開発し公開します。

通常この競争に先行するのは攻撃者です。このようにセキュリティホールが発見されて攻撃可能な状態になってから、メーカーによって修正され攻撃不可能になるまでの期間をゼロデイとよび、この期間を狙って行われる攻撃を「ゼロデイ (ZERO DAY) 攻撃」といいます。

メールなどで送り付けられるマルウェアは、警戒していればある程度防げますが、動画、ウェブサイトやウェブ広告に仕込まれるマルウェアは、特定のウェブサイトを見ただけで感染することもあり、情報が無いままこの方法でゼロデイ攻撃を受けると実質的に防ぐことができません。

被害を少しでも避けるためには、セキュリティ情報サイトや SNS (NISC の Twitter【内閣サイバー (注意・警戒情報)】など) をこまめにチェックして、必要な対応を行うようにしましょう。メーカーがアップデート用のセキュリティパッチを提供するまでの緩和策を公開することもあるので、可能であればそのような対策を実施しましょう。例えば動画系のマルウェアが登場したら動画の自動再生機能をオフにする、スマホ用アプリであればセキュリティホールが

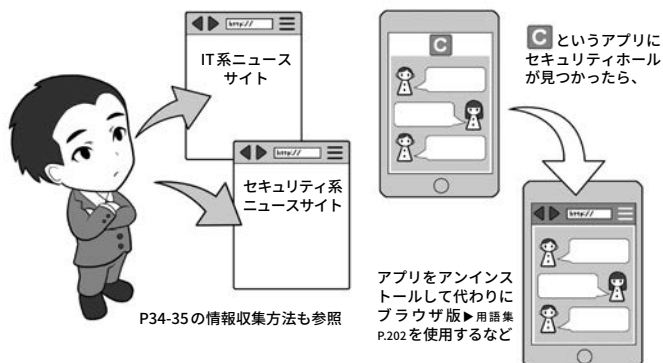
### ゼロデイ攻撃とは？ 対処の例



### ゼロデイ攻撃に対抗するには？

ニュースサイトをこまめに  
見て情報収集

別の手段でセキュリティホールを  
避ける



攻撃者とメーカーのゼロデイ攻撃に関する対応競争は、たいていの場合、攻撃者が先行します。攻撃者はメーカーが気付いていない段階でセキュリティホールの情報を入手し、対象の機種どれか1つでも攻撃に成功するなら攻撃を開始できますが、メーカーは情報を入手し精査した上でセキュリティパッチを開発し、攻撃可能と思われる機種すべてで、セキュリティパッチが正常に動作するか、充分な検証をしてからリリースしなければならないからです。

ですから利用者はそれを前提として備え、ゼロデイ攻撃を想定して対処行動をする必要があります。そうすることが結果として自分を守ることになるからです。

修正されるまでアンインストール▶用語集 P.194 するなどの対応をしましょう。

アプリを提供しているウェブサービスは、アプリが使用できな

い状況でも、ウェブブラウザ▶用語集 P.195 でウェブ版が利用可能なこともあるので、普段からスマホなどでもウェブブラウザ経由での利用に慣れておきましょう。



## 第3章

# SNS・ネットとの付き合い方や 情報モラルの重要性を知ろう

現代では、SNSを通じて、世界中の人たちと簡単につながりコミュニケーションできます。しかし、接する人がすべて自分と友好的であるとは限りません。SNSやネットでよくある危険やトラブルについて知り、対策や家族を守る方法を学びましょう。

### 1 SNSなどのネットとの付き合い方、守り方を知ろう

- 1.1 SNSなどのネットの楽しみ方と気を付けること
- 1.2 SNSやネットの怖さ、こんなことが実際に起こっている
- 1.3 SNSやネットとの付き合い方の基本
- 1.4 ネットいじめに気を付けよう
- 1.5 モラルを逸脱すると炎上を生む
- 1.6 望まない情報流出、流出したら消すことは難しい
- 1.7 こどもにスマホを持たせるとき「スマホ契約書」の提案

コラム1 GPS、位置情報、ジオタグの管理

コラム2 屋外でのゲームを安全に楽しむ。ながらスマホは×！

### 2 インターネットで守るべき法律やマナーを知ろう

- 2.1 アニメ・マンガ・音楽の違法な共有。パクリなどの著作権侵害
- 2.2 ゲームの不正行為はNG／親しくてもプライバシーは守る
- 2.3 クラッキングはクールじゃない！
- コラム3 デマに踊らされない！
- コラム4 法律に違反することをしてはいけません。気軽に考えてはダメ
- コラム5 成人年齢18歳引き下げに伴って注意が必要なこと

### 3 便利なサービスや機能を利用して家族を守ろう

- 3.1 こどもを守る
- 3.2 お年寄りを守る
- コラム6 デジタル遺産相続

## 1

SNSなどのネットとの付き合い方、  
守り方を知ろう

## 1.1 SNSなどのネットの楽しみ方と気を付けること

私たちは、インターネットの普及により、「距離とその移動に必要だった時間が消えた世界」を手に入れることができました。

昔は、遠い国の人と連絡を取り合うには、手紙を書いて何週間も返事を待ったり、電話をかけるにしても料金が高く気軽にかけられなかったり、あるいは顔を見るために旅行するにしても、大変な手間とお金がかかったものです。

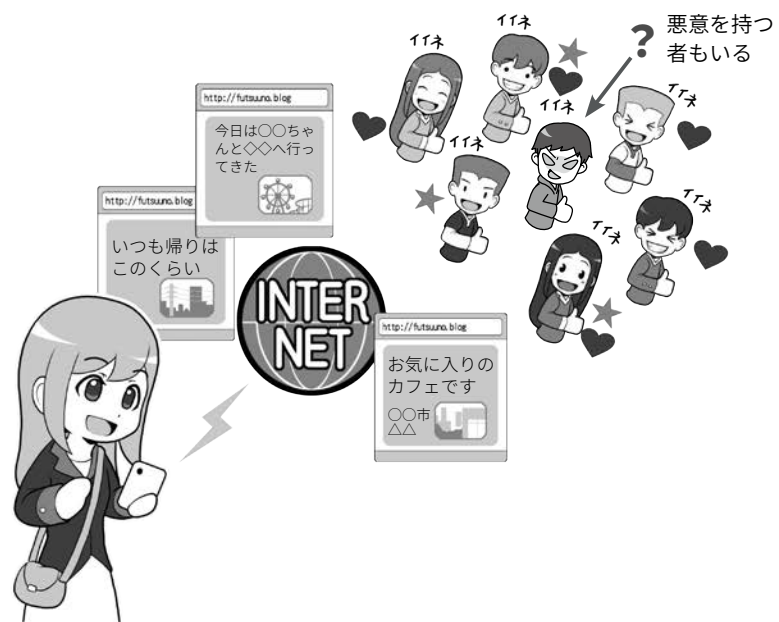
しかし今では、まるで隣に座っているかのようにチャットしたり、SNS▶用語集 P.192 で写真を送りあったり、映像付きのインターネット電話を使えば無料で顔を見ながらコミュニケーションができます。

そして、IT技術の進歩は言葉の壁すらも崩しつつあります。まるで世界が1つになったような時代が訪れ、人の意識そのものが変わっていくかもしれません。

一方、あなたが世界中の人にメッセージを発信するとき、それを受け取る人々の中には悪意を持った人がいることも忘れてはなりません。ネットを使ったコミュニケーションは人と人の意識のつながり合いを容易にしますが、同時に自分の意識の壁の中に、悪意を持った人間が入ってきてやすくなるのです。

私たちは、ネットの世界をよく知って「この時代に合わせた、新しい付き合い方」を作り上げなければならないでしょう。悪意のあるものをしっ

## SNSやネットのコミュニケーションには落とし穴もある



SNSやネットのコミュニケーションは、距離を超えて世界中の人とつながることができます。なに気ない投稿は、多くの人の共感を得るかもしれませんが、その中には、犯罪に使える手がかりを探している悪意を持った人もいます。どうしたら悪意をかわしつつ、SNSやネットを楽しむことができますか？

かりと見分けて、善意のコミュニケーションの世界を作っていくことが必要です。なお、SNSやネット上のリスクは、学校に通う児童・生徒に対しては、昨今のGIGAスクール構想による情報モラル教育▶用語集 P.197 の効果もあり、一定程度は理解が進んでいると思われます。

GIGAスクール構想を推進した文部科学省が告示している小～中～高校の学習指導要領によると、「情報モラル」は学習の基盤となる資質・能力の1つである「情報活用能力」に

も含まれると定め、SNSやネット上のリスクについての理解などを含め、情報モラル教育の重要性が示されています。

一方で、児童・生徒の保護者には、情報モラル教育の重要性やその教育が求められる背景として存在するSNSやネット上のリスクを十分に理解できていない人も少なくないでしょう。こどもと保護者とのサイバーセキュリティに関する知識格差を埋めるためにも、保護者もSNSやネットのリスクは知っておきましょう。

## 1.2 SNSやネットの怖さ、こんなことが実際に起きている

では、SNSやネットではどのようなトラブルに遭う可能性があるのでしょうか。

SNSなどで、実際に会ったことがない同じ年ぐらいの子と友だちになり、どこかで会う約束をしたとします。しかし、待ち合わせ場所に行ってみると来たのは本人ではなくて別の人でした。「〇〇ちゃんが待っているから連れて行ってあげる」といわれ、車に乗せられそうになりました。こんな風に誘拐・略取が行われます。

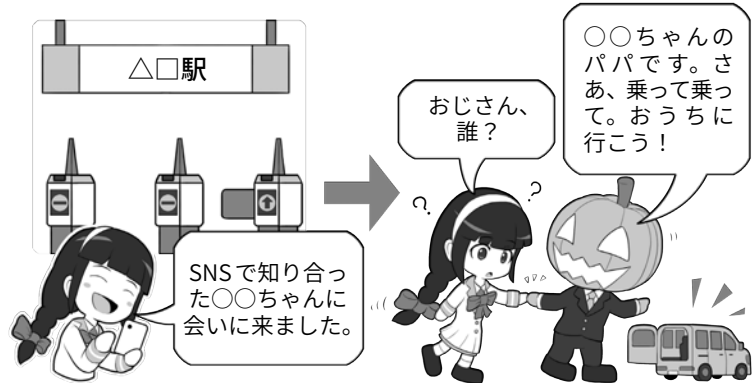
SNSに家の近くや普段立ち寄る場所、自分の写真などを上げていると、その情報からあなたを特定し、リアルなストーカーがやってくるかもしれません。

闇サイトなどを興味本位に覗いたりしていると、犯罪勧誘といって、顔も知らない人があなたを犯罪に誘ってくることもあります。

SNSのグループなどで、周りの雰囲気流され、特定の人物のありもしない書き込みに同調したり、傷つけたり、仲間はずれにしたりする「ネットいじめ」をしたりされたりしてしまうかもしれません。

交際している相手が、「誰にも渡さないから」とあなたの裸の写真を要求してきて、信頼して渡したら、別れた後にその画像がネットに流出してしまうかも。それは、「リベンジポルノ」といって、相手が嫌がらせのために、写真をネットに投稿する行為ですが、その意図がなくても、相手のスマホがマルウェア▶用語集P.203に感染して流出してしまうかもしれません。その写真は、消えない「デジタルタトゥー」(デジタルの入れ墨)

### 誘拐・略取



### ストーカー



SNSで得た情報をもとに人物を特定し、リアルな世界でストーカーされる場合もあります。

### 犯罪勧誘



闇サイトなどと呼ばれる怪しいサイトで、面識がない者同士が集まって、犯罪を行うために仲間を探しています。

### ネットいじめ



ノリでいじめに加わった結果、悲しい出来事が起きてしまったら、自分はそのときどう思うでしょう。

### リベンジポルノ・デジタルタトゥー



元交際相手に、裸の写真をネットに投稿されるかも。ネットに広がった写真は消すことができません。

として、以降あなたの人生に、ずっと影を落とし続けることになるかもしれません。

この他にも、SNSやネットでは、

さまざまなトラブルが発生することがあります。トラブルのことをよく知って、決して巻き込まれないようにしましょう。

### 1.3 SNSやネットとの付き合い方の基本

SNSには、「いいね!」などの他の人からの反応や、コメントをもらうことができる機能があります。「いいね!」をたくさんもらえると嬉しい反面、少ないと気落ちすることもあるでしょう。また、否定的なコメントが来ることもあるかもしれません。人の価値観はそれぞれ違うので、それらに一喜一憂したり、振り回されたりしないようにしましょう。

また、SNSには投稿者にダイレクトにメッセージを送れる機能があるものもあります。知らない人からのダイレクトメッセージには注意しましょう。とくに、実際に会いたいなどの誘いが来た場合は親に相談するなどしましょう。

さらに、多くのSNSでは投稿の公開範囲▶用語集P.196を自由に設定できます。設定範囲によっては友達以外の人が見ることもあるかもしれません。従って、氏名、住所、電話番号、通っている学校などの情報をむやみにプロフィールに掲載しないようにしましょう。個人情報▶用語集P.196を悪用されたりする場合やストーカーなどの被害に合うことも考えられます。

SNSの投稿は、情報や話題の提供など有意義なものです。不特定多数の人が投稿を見られる設定になっている場合は、自分の顔写真や居場所が特定される場合があるので、投稿には十分注意が必要です。また、知らない人だけでなく、友達の顔写真もむやみに投稿すると個人の特定や肖像権の問題が生じる場合がありますので、慎重に行いましょう。

なお、スマホには、こどもに有害と思われるサイトを閲覧できないようにするフィルタリング機能や、ア

#### 「いいね!」が少なくとも気にしない



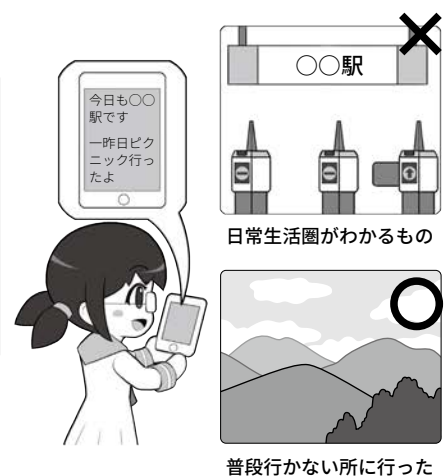
「いいね!」は、人それぞれの主観です。年齢も学校も大人なら仕事も異なります。多様な価値観があることを理解して、「いいね!」の数を気にしないようにしましょう。

#### 個人情報は基本的に公開しない



一度流出した個人情報は、絶対にネットから消し去ることができませんし、ときに個人の居場所を特定する情報になります。悪意がある人にとって、手がかりになる情報はネットに載せないようにします。

#### 個人が特定される情報はSNSなどに投稿しない



自分自身の写真や、日常的な生活圏がわかる情報を投稿しないようにしましょう。友人のみに公開としても、その人が共有したら一般に公開されることもあります。また、デジカメで「位置情報あり」で撮影していると、見なくても写真に位置情報が記録されるので注意しましょう。

プリの使用も含めて、こどものスマホ自体を管理するペアレンタルコントロールの機能があります。これらの機能をこどもの年齢に応じて適切

に使うことで、こどもに対するスマホやネットの安全性をより高めることができます。



## 1.4 ネットいじめに気を付けよう

ネットが学校や家庭に普及する前は、いじめは教室など公共の場所で本人に対して直接行われわかりやすいものでした。しかし、誰もがスマホを持つ現代において、いじめはSNSなどのネット上で行われ表面化しにくだけでなく、巧妙なものになりました。

ネット上で行われるいじめは、SNSなどに悪口を書き込まれたり、皆が入っているSNSのグループから外されたりするなど、ネット技術の進展に伴い形を変えて行われており、大人から見てもわからないようなものが多く存在します。

ネットいじめにあった場合や、ネットいじめをされているのではないかと考えた場合は、保護者や先生に相談することが大切です。また、いじめられている証拠がある場合は、SNSの画面ショットなどの証拠を保存しておくといいです。

また、GIGAスクール構想により学校ではネットワークに接続された端末が配布され、いつでもネットワークを利用することが容易になりました。GIGAスクール構想では、児童・生徒に1人1台の端末を配布し、それらを使いネットワークに接続し、ICT教育だけでなくさまざまな教科の学習を促進させるものです。

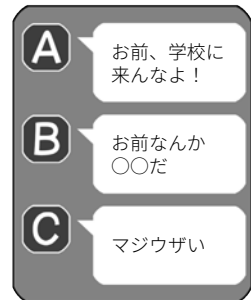
しかし、タブレット端末などの配布により、これらがネットいじめのツールとして使用される可能性も生じます。SNSなどへの悪口の書き込みだけでなく、パスワード▶用語集 P.200 の流出により、ネット上でトラブルになることなども考えられます。従って、学校で配布されたアカウントの管理などもしっかり行うことが大切です。

### いじめは閉鎖された場所で起きやすい

公共の空間では  
人の目がある

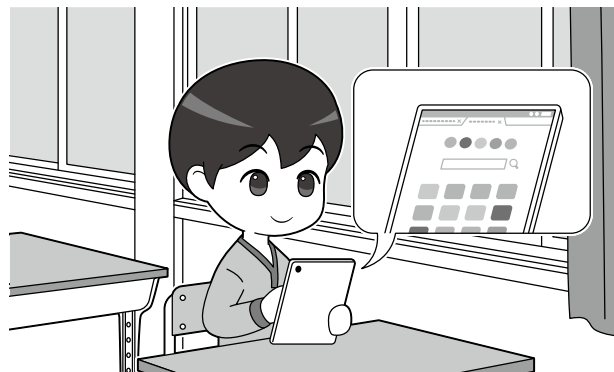


ネットは他人から  
見えにくい



人の目は、ときに抑止力になりますが、ネットの中は人目が少なく、その分いじめは陰湿でエスカレートしがちです。

### GIGAスクールでICT教育環境が充実!!



コロナショックも影響し、2020年から急速に推進されたGIGAスクール構想により、全国の小中学校では児童・生徒1人1台の端末普及が実現しました。

### GIGAスクールの端末は、学校のルールを守り、学習など正しい目的で使う



残念ながら、配布された端末を用いてSNSで他人への悪口を書き込むネットいじめが問題になりました。同じパスワードの使い回し▶用語集 P.201により、勝手に友達のアカウントになりすまし誰が悪口を書いたかわからない事態になるなど、いじめの早期発見が難しくなってエスカレートする可能性があります。

## 1.5 モラルを逸脱すると炎上を生む

ネットのニュースなどを見ていると、「炎上」▶用語集 P.195 という言葉をよく目にします。

炎上とは、特定の人物がSNSなどに投稿した内容が不適切であるとして拡散▶用語集 P.195 され、多くの人から集中的に非難を受けることを指します。

特定のお店に関するいいがかりや嘘の書き込み、飲食店などで働いている人が芸能人のプライベートでの来店を投稿すること、引っ越し業者が業務上知り得た情報で引っ越した女性にアプローチをしたという投稿、あるいは未成年が宴会で飲酒したという投稿などが炎上の例として挙げられます。

多くの場合、世間一般の「モラル」に照らしおかしいと思われるものに対して炎上は発生します。

問題は、その炎上の結果、炎上させた本人が非難されるだけでなく、嫌がらせをされたお店が閉店してしまったり、雇用者である会社が謝罪したりと、周辺に多大なる影響を及ぼすことです。本人も非難を受けるだけでなく損害賠償、名誉毀損で訴えられ、さらには内定が取り消しになるケースもあります。

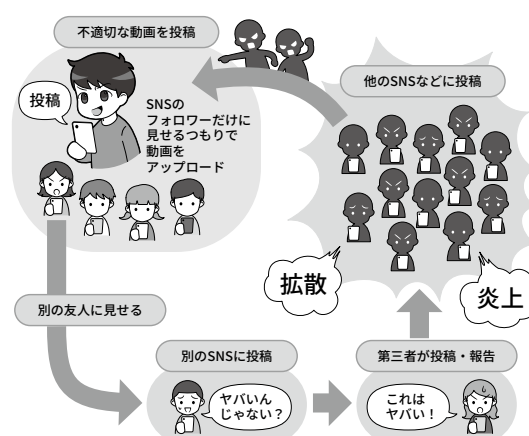
「炎上」をおこさないためには、投稿する人が自分の投稿が広く読まれることを意識した上で、世間が自分の投稿をみたらどう判断するかを考えた上で批判を受けたくないような内容を投稿するか、それに自信がなければ投稿しないことが必要です。

ネットの炎上を見たら、どうしてもそのようなことになったのか、もし、炎上してしまったらどのようなことになるのかを、それを人ごとだと思

### モラルを逸脱することが炎上を生む



### よくある「炎上」の流れ



- ①発信者が自分のフォロワーなどだけが見るだろうと安易に考え不適切な内容を投稿
  - ②投稿を見たユーザーが問題と感じて元とは違う SNS など にその内容を投稿
  - ③フォロワーが多いインフルエンサーが該当の投稿を発見して批判的内容を投稿
  - ④インフルエンサーのフォロワーなどがさらに批判的投稿を行い元の不適切な投稿が拡散
  - ⑤マスコミなどに取り上げられることによりさらに拡散
- といった流れが考えられます。

③の段階にまで至ると、拡散速度が加速度的に増大しなかなか沈静化しません。炎上が一旦生じると、発端の問題投稿をした投稿者の個人情報まで特定され、また、元の投稿の拡散も相まって炎上状態が沈静化した後も、ネット上に問題の情報が残り続けます。

わず自分のこととして考えてみてください。「炎上」はささいなきっかけで起こりうるのです。

また、必ずしも「炎上」ではないかもしれませんが、自分の投稿を多人数のふりをしてもてやはす「自作自演」や、他人のふりをするなりすまし▶用語集 P.200 など、状況によっては犯罪や名誉毀損となる場合があることも知っておいてください。

「軽い気持ちでやった。こんな大変なことになるとは思わなかった」という言い訳は昔からよく聞きますが、一回起こってしまったことにはできません。現実世界とネットでのコミュニケーションの差、SNSの情報拡散の特徴などをよく理解して、後悔のないネットライフを送ってください。



## 1.7 こどもにスマホを持たせるとき「スマホ契約書」の提案

こどもが「スマホが欲しい」と言ってきたとき、こどもとスマホの利用について約束をしていますか？

こどものスマホ利用について、家庭内ルールを定めた上でフィルタリングサービス▶用語集P.201などの保護手段を利用するとトラブルに遭遇しにくいことが、総務省が実施した「我が国における青少年のインターネット利用に係るペアレンタルコントロールに関する調査結果」で明らかになっています。この家庭内ルールを「契約書」という形の約束にすることはどうでしょうか。

「契約書」というと物々しい気もしますが「契約」とは、人と人が守るべき約束ですから、スマホの利用についての約束を口頭ではなくきちんと明文化し、それをお互いに確認合うことで、親もこどももそれぞれの約束を強く認識することができます。

家庭内ルールについては、保護者は「決めている」と思っているのに対して、こどもはそう思っていない、という双方の認識が異なるケースが相当数あることが内閣府の「令和3年度青少年のインターネット利用環境実態調査」で判明しています。この調査結果を考慮すると、ルールを家庭内で確認し合い事前に決めることは重要と考えられます。

ルールを決める際に「契約書」というフォーマルな形で約束をすることで、こども自身、1人前として認められていると感じやすく、約束を守ることへの自覚を促すことにもなります。

契約書の内容は、「ご飯のときにはスマホを見ない」や「午後10時以降はスマホを見ない」といった、各

### 口約束は忘れてしまいやすい？



ルールは決めても、口約束だけで見返せないと、あやふやになってしまいがちです。結果的に感情的なやりとりを生みます。

### 契約書を作り、責任ある人として接する



契約書は固いイメージもありますが、ルールをときどき見返すことができる他、言った言わないにならないというメリットもあります。

なにより相手を責任ある人間としてあつかうことで、ルールを自ら決めたことの自覚と守ることへの自律を促しましょう。

ご家庭における重要なルールとともに、こどもがネットでトラブルに遭わないようにするためのルールを書

いておくといいでしょう。

例えば、「面と向かって言えないことはSNSでも言わないこと」「SNS



には誰に読まれても困らないような内容をアップすること」といったルールは、SNS上で、友だちしか読まないと思って他人に対する過激な誹謗中傷や名誉毀損を行うことを避けるために役立ちます。また、「不特定多数に見られて困る恥ずかしい写真は、頼まれても絶対送信したりアップしたりしないこと」といったルールは、ネット上ではよい人に思える相手に恥ずかしい写真を送ってしまったのちに、その写真をネット上で公開されたり、その写真を元に脅迫されたりするなどの被害に遭うことを防ぐために重要です。

契約書を作るにあたっては、親・こどもの双方が納得できるようにしっかりと話し合うこと、こどもが守れるルールを作ること、契約書のルールは具体的な内容にすることが重要です。あわせて、ルールを守れなかった場合についても、どうするかきちんと決めておきましょう(契約ってそういうものですね)。

「家庭のルール」を相談して決める際には、文部科学省が情報モラル教育推進事業として公開している「話合っていますか？家庭のルール」という保護者向け教材が参考になります。家庭内でルールを作ることの重要性、ルールを作るときのポイント、そして「家庭のルール」チェックリストなどがまとめられています。

また、スマホ契約書は一度作ったら作りっぱなしでは不十分です。こどもの成長に合わせてルールを見直し、契約書を更新していくことも、実効性のあるルール作りのためには必要です。

## 家庭のルールを明文化した契約書やチェックリストを作成することが重要

### 「家庭のルール」チェックリスト

インターネットは生活に不可欠なものになりました。次の時代を生きる子供たちが、新たな機器やサービスに対応し、安全に賢くインターネットを利用するために、「家庭のルール」を作りましょう。

- ☐ 「ルールがトラブルから自分自身を守ってくれる」ことをきちんと伝える。
- ☐ お互いに納得できるよう、話し合って作る。
- ☐ 子供が守れるルールを作る。
- ☐ 具体的なルールを作る。
- ☐ 守れなかったらどうするか決めておく。
- ☐ トラブルがあったら保護者に相談するよう決めておく。

ルールを作ったあとも・・・

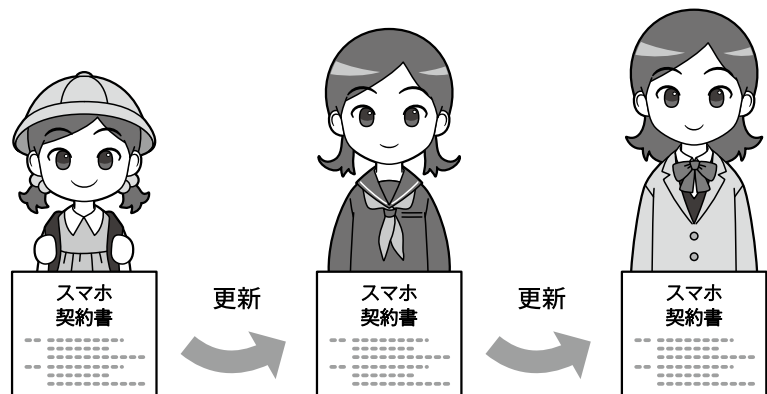
- ◎ 子供の成長に合わせてルールを見直しましょう。
- ◎ 生活リズム等の変化に合わせてルールを見直しましょう。

「家庭のルール」を決めるには、文部科学省の保護者向け教材「話合っていますか？家庭のルール」にある『「家庭のルール」チェックリスト』が参考になります。

文部科学省「話合っていますか？家庭のルール」～「家庭のルール」チェックリスト

[https://www.mext.go.jp/component/a\\_menu/education/detail/\\_icsFiles/afieldfile/2016/06/07/1371802\\_3.pdf](https://www.mext.go.jp/component/a_menu/education/detail/_icsFiles/afieldfile/2016/06/07/1371802_3.pdf)

## スマホ契約書はこどもの成長にあわせて適した内容に更新する



スマホ契約書は一度作ったら作りっぱなしでは不十分です。こどもの成長に合わせてルールを見直し、契約書を更新していきましょう。

2022年5月総務省「我が国における青少年のインターネット利用に係るペアレンタルコントロールに関する調査結果」

[https://www.soumu.go.jp/menu\\_news/s-news/01kiban08\\_03000375.html](https://www.soumu.go.jp/menu_news/s-news/01kiban08_03000375.html)

内閣府の調査研究「令和3年度青少年のインターネット利用環境実態調査 第2章第1説(4)」

[https://www8.cao.go.jp/youth/kankyouto/internet\\_torikumi/tyousa/r03/jittai.html/index.html](https://www8.cao.go.jp/youth/kankyouto/internet_torikumi/tyousa/r03/jittai.html/index.html)

## コラム.1 GPS、位置情報、ジオタグの管理

私たちが普段なにげなく使っているスマホは、相当に高性能で、10数年前ならばすべて別々の機器だったものが、まとまって1つの小さな機器に収まっています。

例えば、電話、音楽プレイヤー、デジカメ、ビデオカメラ、そして、GPS▶用語集 P.191 レシーバーなど。

とくに昔は、GPS衛星からの電波をキャッチして、緯度経度で構成される位置情報を測るには、大きな専用のGPSレシーバーが必要でした。今はスマホの地図アプリを開いて「現在地」を押せば、即座に自分がいる場所を示してくれます。

しかし、便利になった代わりに、油断すると意図せずそれらの位置情報を公開してしまっていることもあります。

例えば、スマホで写真を撮影するときに位置情報を記録するようにしておくと、撮影場所の情報が「ジオタグ」という形で写真に保存されます。

ジオタグが記録されている写真を、写真アプリなどで見返すと、地図上の撮影したポイントに写真を配置して見ることができ、時系列順に並んだたくさんの写真からわざわざ探さなくても、思い出の場所で撮った写真を即座に見つけることができます。

これは便利ですが、写真にジオタグをつけたままSNSに投稿すると、SNSのサービスによってはジオタグが削除されず位置情報がわかる設定で公開されることもあり得ます。その写真が自宅で撮影したものであると、世界中に自

### 写真には位置情報が含まれることも



プロパティ

GPS

緯度 35.394348  
経度 138.733276  
高度 2305m

スマホによっては購入時の設定で、写真に位置情報を記録するようになっている場合もあります。必要なければ機能をオフにしましょう。

### 位置情報は思い出を見返すのに便利



地図表示



画像アプリによっては地図上に写真が表示され、思い出の場所を拡大すると、そこで撮影した写真を見ることができます。写真を一から探さなくてよいので便利です。

### 位置情報はストーカーの手がかりになる



位置情報  
発見

写真に付加された位置情報、投稿時の位置情報だけでなく、場所の名前や、場所が特定できる写真からはあなたの居場所が分かります。ストーカーにとっては絶好の手がかりになるので、投稿前後に必ずチェックしましょう。

宅の場所が公開されてしまうのです。

また、位置情報はSNSの投稿時に位置情報を公開する設定にしておくと、文字だけの投稿をしたつもりでも、写真を撮った場所まで文字で公開されてしまいます。

生活圏の位置情報を公開してしまうトラブルは、GPSにまつわるものだけではなく、普段立ち寄る店の名前を投稿したり、周りの風景が映り込んだ写真を投稿したりするだけで、いともたやすく「撮影場所が特定される」ことがあり

ます。

そして、これらの「位置情報」もしくは「位置情報に相当する情報」は、ストーカーにとっては絶好の手がかりになります。

ネットは知らない人と「距離とその移動に必要な時間」を超えて知り合える場所ですが、トラブルが発生すれば、それは距離を越えて現実世界の我が身に即座に襲いかかってきます。

位置情報を含む個人情報の管理は、しっかり行いましょう。

## コラム.2 屋外でのゲームを安全に楽しむ。ながらスマホは×！

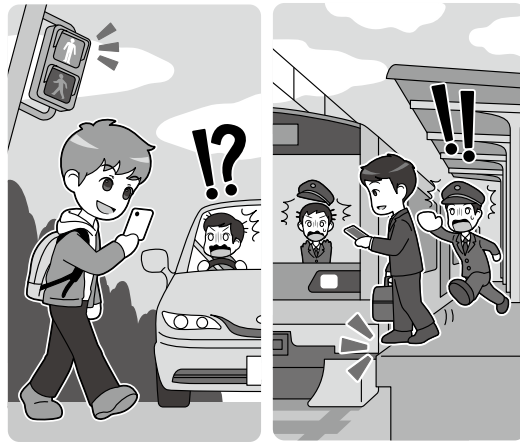
スマホの代表的なゲームジャンルの1つに「位置情報ゲーム」があります。スマホの位置情報機能を活かして、全国の駅巡り、カメラと組み合わせて特定の場所にしか現れないレアモンスターの捕獲、ご当地アニメキャラクターと写真撮影といったことができ、人気を博しています。しかし、カメラを併用することも多いので、遊ぶときは注意が必要です。

まず、屋外では「ながらスマホ」「歩きスマホ」でゲームをするのは危険なのでやめましょう。自分は大丈夫と思っていても、歩きスマホは大変危険な行為です。歩いているうちに車道に出て事故に遭ったり、駅のホームから転落することもあります。また、歩きスマホをしている人を避けようとして、自転車や自動車に乗っている周囲の人が事故を起こしてしまう可能性もあります。歩きながらのゲームプレイによる、事故やトラブルも多く起きています。

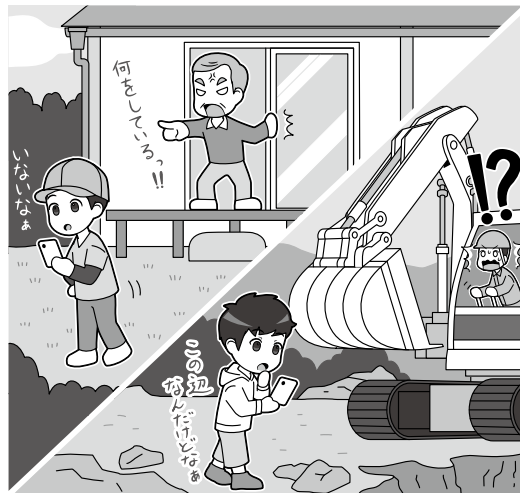
ましてや自転車や自動車を運転しながらのスマホ操作は言語道断です。運転中のスマホ操作は、道路交通法によって禁止された行為で破った場合は罰則・罰金が定められています。また、ゲームに熱中しすぎ気付かないまま私有地に入り込んでしまうと「不法侵入」にあたります。危険な場所に入り込んでしまえば、不注意からケガをしてしまう可能性もあります。危険な場所には、ゲームのプレイエリアが設定されていても、近づかないでください。

ただ、位置情報ゲームは使い

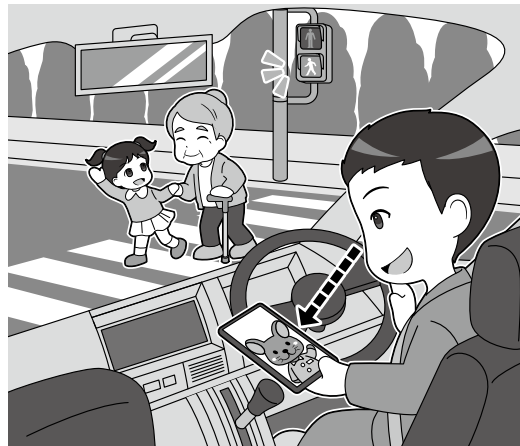
### 歩きスマホは自分も周りの人も危険



### 私有地や危険な場所には入らない



### 運転中のスマホはダメ。車は凶器になります



方によっては観光振興も期待され、今後も多くの人が楽しむでしょう。

プレイする際は、交通ルールやマナーを守り安全に遊びましょう。



# インターネットで守るべき法律やマナーを知ろう

## 2.1 アニメ・マンガ・音楽の違法な共有。パクリなどの著作権侵害

インターネットは、基本的にさまざまなものを共有する場です。しかし、著作権者の許可を得ずに、ネットにアップロードされた、映画、アニメ、テレビ番組、音楽、マンガなどの作品を、そうと知ってダウンロードするのは違法行為です。

また、同様に、上記のような作品を著作権者の許可を得ずにインターネット上にアップロードして配信する行為も違法です。

違法アップロード・ダウンロード  
▶用語集 P.194 は作品が生み出される環境を破壊し、結果として新しい作品が生まれなくなります。コンテンツを利用するときは許可を得て公開されているものを利用しましょう。例えば、音楽の場合はエルマーク、漫画などの書籍はABJマークがついているサイトは、適法に許可が得られているサイトです。(エルマーク <https://www.riaj.or.jp/leg/lmark/> ABJマーク [https://aebs.or.jp/ABJ\\_mark.html](https://aebs.or.jp/ABJ_mark.html))

ネットをよくいわれる「パクリ」▶用語集 P.200 も基本的には著作権侵害▶用語集 P.199 です。

例えば、他人がSNSに投稿した写真や文章を、自分のもののふりをして勝手に投稿することや他人がウェブ▶用語集 P.194 で発表した小説や写真などの、一部もしくは全部を自分のもののように偽って公開することも著作権侵害であり、SNSによっては利用規約違反としてアカウント

### 違法アップロード、ダウンロードは刑罰の対象にも……



\*1: 有料の作品が違法にアップロードされているものと知っていた場合

### 他人の投稿や作品を盗む「パクリ」



を停止される場合もあります。

パクリで一瞬だけ注目を集めても、いずれ身元が特定されるなどして「パクリった人だ」とネットに記録されて

しまったらいやですね。ちなみに、自分のもののように偽らなくても、勝手に転載したら著作権侵害です。



## 2.2 ゲームの不正行為はNG／親しくてもプライバシーは守る

ゲームの不正コピー▶用語集 P.202 やチート行為▶用語集 P.198 はやってはいけません。規約違反ですし、場合によっては犯罪として摘発されます。「自分1人ぐらいやっても大丈夫」という人たちが増えると、ゲームそのものの環境を破壊してしまうことになります。

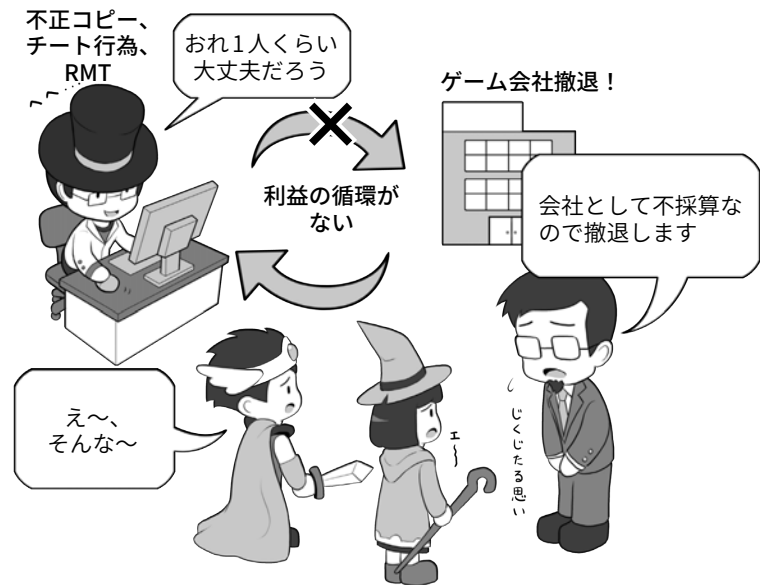
ゲームを作る人はゲームを売ることによって利益を上げ、生活をし、また、新しいゲームを世の中に生み出してくれます。この利益の循環があるからこそ、ゲームを遊ぶ側は楽しい時間を過ごせるのです。しかし、誰かが不正行為でこの「利益の循環」を回らなくしてしまうと、やがてゲームを作る人々は生活できなくなり、結果としてゲームがこの世に生み出されなくなってしまいます。

楽しみのある世界がよいですか？ ない世界がよいですか？ゲームを作る側も遊ぶ側も信頼関係があれば楽しい世界ができていくはずですよ。

信頼関係は普段の生活でも大切です。例えばプライバシー。あなたが席を立っている間に勝手にスマホの中身を見られたり、親にあなたがパソコンに保存している日記を見られたりしていただどう思いますか。とくに「信頼している」人にこのようなことをされると深く傷付きますよね。

親しい仲であってもプライバシーは大切です。とくにスマホやパソコンはプライバシーの固まりです。親しいからこそ、プライバシーを尊重し、信頼関係を守りましょう。

### ゲームの不正行為は犯罪になることも…



不正コピー、チート行為、RMT（リアルマネートレード）▶用語集 P.191 など、ゲームの販売や運営を妨げたりする行為は、場合によっては犯罪として摘発されますが、積み重ねてゲームを生み出す会社やシステムの崩壊を引き起こしてしまうことも問題です。

その結果、みんなが楽しめる世界が奪われてしまうのです。利用者を信頼している制作者の人たちを裏切ってはいけません。

### 恋人や家族の間でもプライバシーは大事、でしょ



恋人や親であっても、スマホの中を勝手に見たり、内緒でパソコンを開いて勝手に日記を見る行為はプライバシーの侵害です。とくにスマホやパソコンはプライバシーに関する情報が詰まっています。これを勝手に見られたら、「信頼関係」に対する重大な裏切りと感じるでしょう。親しいからこそ、プライバシーを尊重し、信頼関係を守りましょう。

## 2.3 クラッキングはクールじゃない！

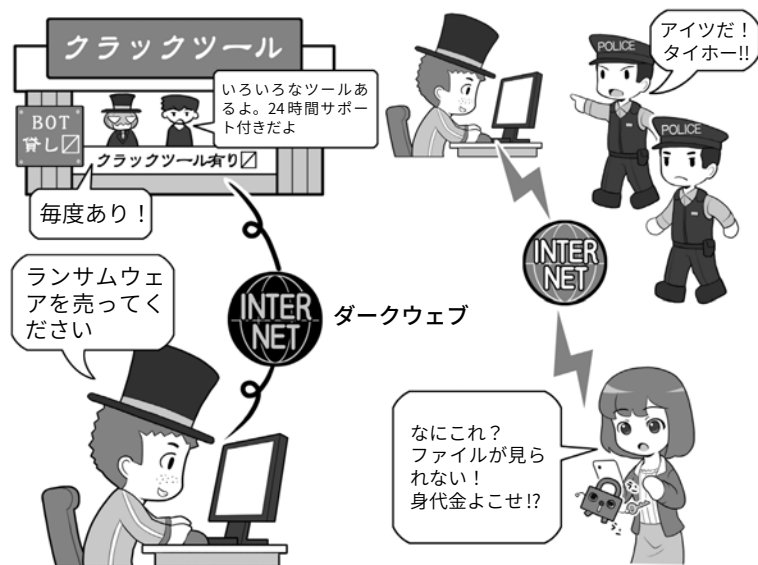
インターネット上には、「ダークウェブ」▶用語集 P.198 という通常であればアクセスすることがないようなサイトがあります。そこでは、アンテナありとあらゆるものを売るマーケットが存在し、悪意のハッカー▶用語集 P.193 によるクラッキング▶用語集 P.196 用ツールの販売や、DDoS 攻撃▶用語集 P.190 のためのゾンビ化した機器群貸出しなどがされたりしています。

近年、若い子どもたちがここに足を踏み入れ「インターネットは匿名だからばれないだろう」とツールを入手して、ランサムウェア▶用語集 P.203 によるサイバー攻撃や不正送金▶用語集 P.202 などを行った事例が報告されており、行為者が逮捕された例もあります。そのようなサイトで入手したツールなどを使う行為の多くは、不正アクセス▶用語集 P.202 禁止法違反、ウィルス作成罪、業務妨害罪などの刑法犯に該当する行為です。でもばれないと思ってやってしまうのです。

果たして、それは本当にばれないのでしょうか。インターネットは、当初悪意が存在することが想定されていない空間でした。しかし、そこに悪意が芽生え、犯罪に利用されるようになった結果、各国の捜査機関も日々こういった犯罪に対応する技術力を向上させています。事件と報道されるのは、捜査機関が地道な解析などで犯人を追い詰め特定しているからです。匿名だからばれないということはないのですね。

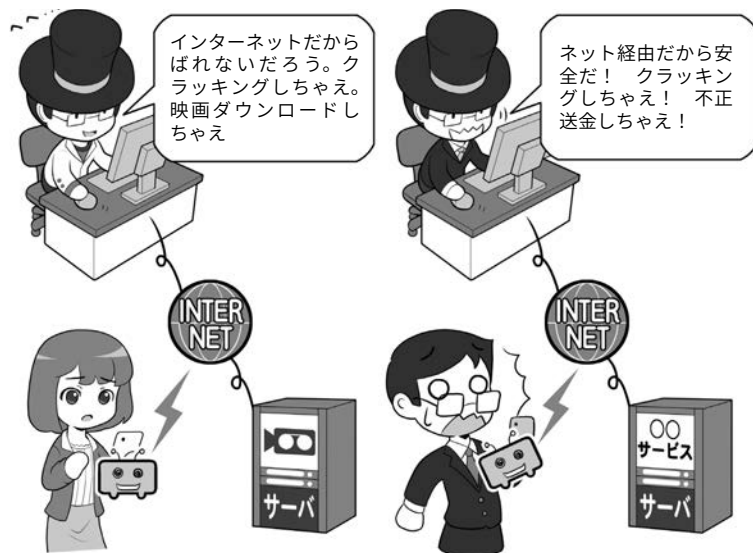
「有名になりたかった」「腕試しをしたかった」「小遣い稼ぎで」そういう言い訳をしても、その行為は単な

### クラッキングツールに手を出さない



現実世界でもネットでも、広く知られている「安全でない場所」や「怪しい場所」は、当然のことながら捜査する側もよく調べ、必要な対策を講じています。「匿名性が高い」はずなのに「捕まったこと」が記事になるということは、なにを意味するでしょう？ ネットでも危険場所には近づかないようにしましょう。

### インターネットだからばれないと思うのは……



本人は軽い気持ちで始めているつもりでも、クラッキングはさまざまな法律や利用規約に違反します。そして、見つからないと思っていても、現実世界に生きる私たちは、現実世界に生きている痕跡を完璧に消すことはできません。

る犯罪です。有名になったところで、その悪名がネットに刻まれるだけで誰も尊敬はしてくれません。実名が流出してその後の人生にずっと影響し続けることだってあるのです。

それよりも、腕と技術力で多くの人々をハッピーにし、ネットの偉人として名前を刻む方が「かっこいい」のではないのでしょうか？





サイバー犯罪というと、それなりの年齢の悪意のハッカーを想像するかもしれませんが、実は非常に若い子どもたちが行い、その結果児童相談所に通告されたり、書類送検されたりしている例もあります。

コンピュータやスマホを使う際には、見てはいけないウェブサイト▶用語集 P.194、危険なサイトへのアクセスを防ぐフィルタリングを利用するだけでなく、こういうことをしてはいけないのか、そういう行為は法律に違反する場合もあることを家族で話し合っておきましょう。下記の例などを参考に、これが他人ごとではなく身近に起こる可能性があることとして、家族で話し合ってみてください。

#### ■アカウント乗っ取り

小学4年生の女子児童が、会員制の交流サイトでサービス上の通貨の提供を条件に、別の女子中学生のID▶用語集 P.191 とパスワードを聞き出し、本人になりすましてログイン▶用語集 P.204 し、その女子中学生のアカウントを乗っ取ったとして不正アクセス禁止法違反の容疑で補導され、児童相談所に通告された例があります。

#### ■ウイルス保管と提供

動画サイトなどに掲載されていた動画を参考にコンピュータウイルスを作成、これを保管、提供したなどの理由で、小学3年生の男子児童が不正指令電磁的記録提供などの非行内容で児童相談所に通告されています。またこれを

#### 他人のアカウントへの不正なログインや乗っ取りをした場合



##### 不正アクセス禁止法

不正アクセス行為の禁止

第3条、第11条  
→ 3年以下の懲役または  
100万円以下の罰金

#### コンピュータウイルスの作成や保管をした場合



##### 刑法

不正指令電磁的記録作成等

(作成、提供、供用)  
第168条の2  
→ 3年以下の懲役または  
50万円以下の罰金

(取得、保管)  
第168条の3  
→ 2年以下の懲役または  
30万円以下の罰金

#### 児童ポルノの所持・提供をした場合



##### 児童買春、児童ポルノ禁止法

児童ポルノ所持、提供等

(所持)  
第7条第1項  
→ 1年以下の懲役または  
100万円以下の罰金

(特定少数者への提供)  
第7条第2項  
→ 3年以下の懲役または  
300万円以下の罰金

ダウンロードした他の小学生も不正指令電磁的記録取得の非行で児童相談所に通告されています。友だちを驚かせたいという軽い気持ちだったようです。

#### ■同級生の少女の裸の画像を拡散

同級生が高校生の少女に裸の

画像や動画を撮影させ、これをSNSに投稿することを強要し、そののち拡散した例で、関与した男女の生徒は、児童買春・児童ポルノ禁止法違反(製造、提供など)の疑いで書類送検されています。



## コラム.5 成人年齢18歳引き下げに伴って注意が必要なこと

2018年6月に成人年齢に関する民法が改正され、2022年4月1日から施行されています。その結果、成人年齢が20歳から18歳に変更され、2022年4月1日以降は、18歳になると成人になり、また、同日18歳、19歳になっていた人は、この日をもって成人となっています。

さて、成人するとなにが変わるのでしょうか。すぐに思いつくのは、飲酒や喫煙、ギャンブルなどがありますが、これらは、成人年齢が変更されても20歳以上でなければできないとされたままで変更はありません。最も大きな変化は、18歳以降は「親権者の親権に服さなくなる」ことです。

未成年者は、親権者の同意なく契約行為ができませんが、今回の改正で、18歳になれば成人になりますから自らの意思で契約行為をすることができます。

例えば、携帯電話を利用するためには回線の利用契約が必要ですが、未成年者は単独で契約ができないため、保護者が利用者を未成年として契約するか、保護者の同意を得て未成年自身が契約することになります。現在は、18歳以上ならば自身が単独で契約できます。また、青少年インターネット環境整備法で携帯電話会社に提供が義務付けられているフィルタリングも、現在は18歳ならば自分の意思で解除を行うことができます。

ソーシャルゲーム、オンラインゲームでの課金やオンライン通販などでの購入も契約行為です。親権者の同意のない課金は、未成年者による契約を理由に取消を申し出ることが可能でしたが、現在は18歳になれば成人ですので、今まで未成年取消が可能だった18歳や19歳の人は、未成年を

理由として取り消すことができません。18歳以上の人は、ゲームなどで課金する場合、自身で課金額などを確認し、支払える範囲内に収めておくよう心掛ける必要があります。

高齢者だけでなく成人したばかりの若者をターゲットに、情報商材やマルチなどの儲け話でだましたり違法行為をさせたりするトラブルやSNSなどで甘い言葉や人間関係を作って勧誘するような手口が、国民生活センターから報告されています。18歳以上の人はこのような商法に関しても成人として扱われることになり、このような手口による商法が従来よりもより低年齢層にターゲットが広がるおそれもあります。日頃からこうした甘い言葉や見知らぬ人からの誘いには注意しておきましょう。

### 18歳成人化の対象者

対象者	成人になる日	成人年齢
2002年4月1日以前の生まれ	20歳の誕生日	20歳
2002年4月2日～2003年4月1日生まれ	2022年4月1日	19歳
2003年4月2日～2004年4月1日生まれ	2022年4月1日	18歳
2004年4月2日以降の生まれ	18歳の誕生日	18歳

### 変わったもの・変わらなかったもの

変わったもの	変わらなかったもの
<ul style="list-style-type: none"> <li>・携帯電話の契約</li> <li>・ローンを組む</li> <li>・クレジットカードをつくる</li> <li>・賃貸契約を結ぶ</li> <li>・10年有効のパスポート取得</li> <li>・結婚 など</li> </ul>	<ul style="list-style-type: none"> <li>・お酒を飲む</li> <li>・タバコを吸う</li> <li>・競馬、競輪、オートレース、競艇の投票券(馬券など)を買う</li> <li>・大型・中型自動車運転免許の取得 など</li> </ul>

# 便利なサービスや機能を利用して家族を守ろう

## 3.1 こどもを守る

こどもをインターネット関連の犯罪から守るには、理由を述べずにあれもダメこれもダメと頭ごなしに禁止せず、まず可能な限りどういった犯罪がどのように行われるのかを知らせましょう。

こどもたちが犯罪に当たる行為をするとき、本人たちはそれが「犯罪になると思っていた」あるいは「知らなかった」という例もあります。知ることが抑止することにもつながります。

サイバー犯罪に遭うという視点からも、問題点や危険性、また、それによってどれぐらいの範囲にトラブルが広がるのか、きちんと共有することが必要でしょう。

その上で、セキュリティソフト▶用語集 P.198 やフィルタリングサービス、緊急時のための位置情報共有の必要性と一緒に確認しましょう。

いざというとき、こどもを助けに行くためには、位置情報は非常に有効な手段です。一方、こどもたちは過度に位置情報に関する追求されると、共有を切ってしまうかもしれません。こどもでもセキュリティの設定などはすぐに変更してしまうでしょう。こどもに対しては、セキュリティの必要性をわかりやすく説明しましょう。とくに位置情報の共有は監視のために使わないことを約束し、そして、約束を守りましょう。

また、こどもからルールの変更やどうしても見たいウェブサイトなどを言い出しやすい雰囲気を作り、そ

### 本当は怖いインターネット

理由をいわずに禁止するのは命令



ネットでなにが起るかを一緒に見る



頭ごなしに禁止せず、インターネット関連のトラブルの実例を見ながら、なぜダメなのかを「理解」しあって共通の認識を作ります。こどもだけでは、対処できないトラブルがあることを知ることが重要です。

自分だけは大丈夫と思わせない

自分だけは大丈夫なんてことはないんだよ。なにもなくても犯罪には遭うけど、犯罪が起こる場所に近づくより高確率で遭ってしまうよ。

なにかあってからだと、守れる確率がぐっと減るんだよね。どうしたらいい？



保護者機能や位置情報を活用する

危ないサイトをフィルタリングサービスでブロック

どうしても見たいサイトがあるなら、パパかママと見ましょう。

普段はチェックとかしないから、情報共有をしましょう。遅くなるときはSNSで連絡が取れるようにしてね



意識を共有したら、実例を示してこどもたちに答えを出してもらいましょう。自分で出した答えは自らのルールとなるからです。

れについて一緒に話し合って勉強する姿勢を示しましょう。スマホやIT機器は絆を断絶するためのツールではなく、より太く結ぶためのツールなのです。

スマホが使えないほど幼い子どもたちを守るサービスや機器も、いろいろと登場しています。

学校を離れたときや駅を通過したときに、親のスマホにメールが送信される見守りメールサービスや、簡単なスマホとGPSと防犯ブザーが合体したキッズケータイは、こどもたちが意識しないで使え、あるいはシンプルな操作方法を理解したら、いざというときの強い味方になります。

また、ある程度スマホの操作をすることができる年齢になったら、位置情報を送信したり、必要な情報をメールやSNSを通じて共有する方法を、一緒に覚えるのもよいでしょう。

位置情報共有アプリ▶用語集P.194は便利ですが、悪用されストーカーなどの被害に遭う可能性もあり、刺傷事件に至ったケースもあります。位置情報を共有するのは、こどもが幼いうちは親のみにしておくようにするとよいでしょう。また、ある程度の年齢になっても不用意に必要以上の人と位置情報の共有をしないことが重要です。

なお、現在は建物の中で迷子になると位置情報や何階にいるかなどの情報は共有できませんが、今後地下街や建物内などにビーコン(Beacon)と呼ばれる装置が普及することで、屋内でも位置情報の交換が可能となると考えられます。

また、どこかではぐれても、電車やバスの乗り換え案内や徒歩ナビゲーションなどのアプリを利用して、家に帰り着く方法をこどもと一緒に学びましょう。

## 安全を守るさまざまな方法

### 見守りメール



見守りメールは、鉄道会社や一部の学校などが提供しているものがあるので、自分が住んでいるエリアでサービスが行われているかを調べてみるとよいでしょう。

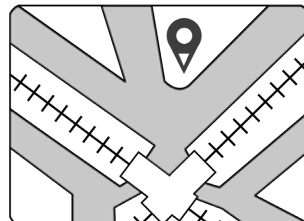
### GPS付きキッズケータイ



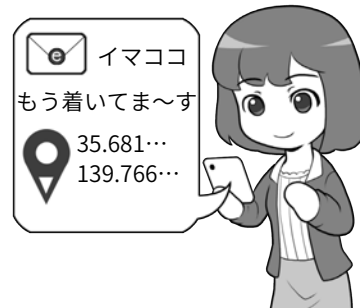
連れ去りや変質者に遭遇したときに使用する、防犯ブザーと簡単な通話機能が一体になったスマホです。簡単な操作で登録された特定の人物への通話なども可能です。

### 位置情報の送信

#### 地図アプリ

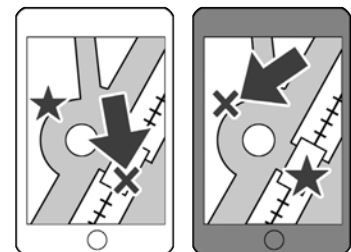


位置情報をメールやアプリで送信



地図アプリの位置情報共有機能を利用して、メールやメッセージアプリ▶用語集P.203から現在地を簡単に相手へ送信できます。受信した相手も自分のスマホの地図アプリを起動すれば位置を確認できます。

### 位置情報共有アプリ



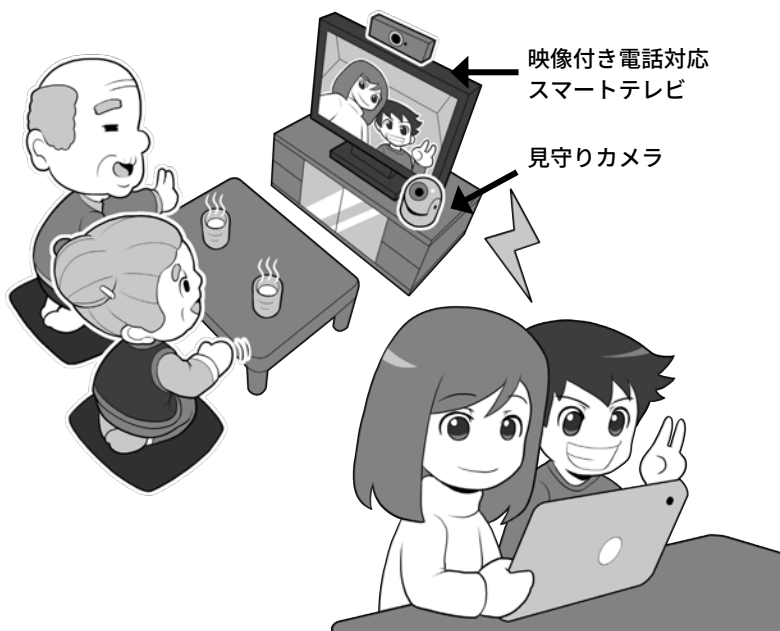
位置情報共有アプリは位置情報を相手へ送信する手間を省いて共有でき便利ですが、不用意に必要以上の人と位置情報の共有をしないことが重要です。

## 3.2 お年寄りを守る

離れて暮らしているお年寄りと連絡を取り合うのに、テレビ電話機能に対応したスマートテレビや大きなタブレット、液晶付きスマートスピーカーをプレゼントして、ときどき映像付き電話をして声だけでなく顔を見せるのもよいでしょう。また、1人暮らしのお年寄りの見守りのために、よく相談をした上でウェブカメラの設置をしたり、毎日部屋の中を動いて電化製品やガスを使用しているかをメールで連絡してくれるサービスも存在するので、こちらも相談し、納得してもらった上で利用したりするのもよいでしょう。一番よいのは会いに行くことですが、離れて住んでいて頻繁に会えないならば、そういうときこそインターネットの「距離とその移動に必要だった時間が消せる」という能力を生かしましょう。

また、「自分は大丈夫」と思っているお年寄りほど、あっさりと振り込め詐欺などに引っかかってしまうものです。振り込め詐欺は電話で顔が見えない状況で、相手を不安に陥れ正常な判断ができなくなることを利用しています。これに対抗するために、例えば、ご両親に連絡するときは、通話アプリのTV電話機能を使うと決めておけば、顔が見えない状況で丸め込まれ、だまされることを回避できるかもしれません。そのテレビ電話機能のためではありませんが、お年寄りには使いやすい簡単操作のスマホを渡すのも1つの方法です。または、いざ操作を勉強する段になって教えてあげやすいように、自分が持っているものと同じ機種を渡しておくのも1つの考え方です。

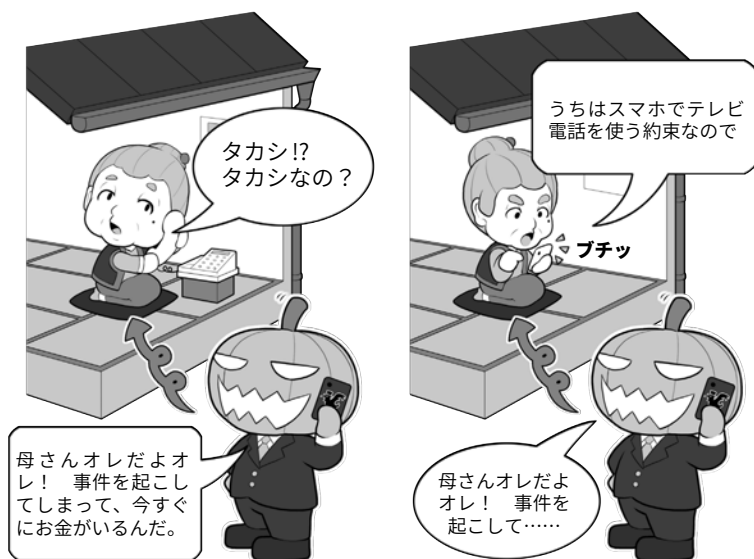
### 映像付き電話やITサービスの活用



お年寄りにとってこどもや孫たちの顔を見るのは、なによりの楽しみです。会いに行きあげるのが一番ではありますが、なかなか訪ねて行けないときは、顔を見てコミュニケーションを取れるツールを活用しましょう。

また、1人暮らしのお年寄りに万が一のことがあったときのために、日々生活状況を確認められるサービスも存在しますので、利用を検討してもよいでしょう。

### IT機器を使った振り込め詐欺対策



電子機器の操作に不慣れなお年寄りでも、スマホの電話機能ならよく使うでしょう。こどもや孫から連絡を取るときは必ずテレビ電話を用いるという方法を使えば、顔が見えない状況で不安に陥れる「振り込め詐欺」などの予防にもなります。同じスマホを渡してあげれば、操作を教えることも簡単です。



ご両親の海外旅行時に、きちんと目的地に着けているか、迷ったりしていないか心配な場合は、事前に相談して位置情報共有サービスや移動履歴が残るサービスを設定して旅に出てもらいましょう。

こうすることで、今どこにいるかを確認できるので、予定どおりに旅行しているかもチェックできます。

また、仮に旅先で迷子になってしまっても現在地がすぐわかれば、どのようにしたらよいかのアドバイスも的確にできるでしょう。

そのようなことはあまりあってほしくありませんが、もしスマホを紛失したり盗られたりした場合も、操作するための情報を共有しておけば、スマホをロック▶用語集P.204したり所在地を確認したりできます。

認知症を患っているお年寄りは、家族の見えていないときに外に出て徘徊し、事故に遭ってしまふことがあります。

また、一緒に外出した後で目を離した隙にいなくなってしまう、本人も自分がどこにいるのかわからず、その結果、行方不明になってしまうケースもあります。

そういった場合に備えて、GPS発信器を使った位置情報サービスを契約したり設定したりしておく、間をおかず探し出すことができます。

もちろん目を離さないことが重要なのですが、ご自身にリカバリする能力がない状況では、万が一に備えた方が安心でしょう。

持ち慣れない機器を持つことを嫌がるお年寄りの方も少なくないので、機器を携帯してもらう際に工夫は必要ですが、事故などを未然に防げる可能性が少しでも高くなるならば、検討してみるとよいでしょう。

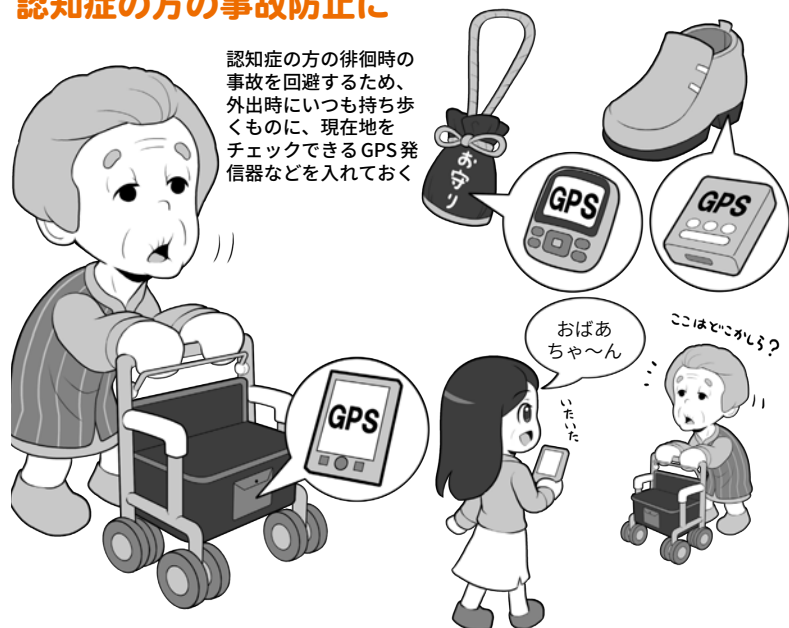
## 位置情報の共有(安否確認)



スマホの位置情報の共有設定をし、現地でもインターネット接続サービスを利用できるようにしておくと、世界中どこにいても現在地を確認することができます。年輩の方自身が位置情報を使いこなせなくても、電話やSNSのメッセージ機能などを使ってサポートすることができます。

※現地でデータ通信できるように、データローミング▶用語集P.199の利用や海外用のSIM▶用語集P.192を手配する場合は、渡航前に準備や設定を済ませておきましょう。また、現地に着いたときに確認すべき事項を紙などに書いて、事前に説明しておきましょう。海外で購入したSIMの使用は最初の設定をしないと、インターネット接続もできない場合がありますので注意が必要です。

## 認知症の方の事故防止に



普段押して歩くカートや、お守りに入れて持たせたり、物を持ちたがらないお年寄りには、靴の中に入れられる機器も存在するのでそのようなものを利用したりします。しかし、これらはなにかあったときのバックアップの手段で、普段から目を離さないことがなにより大切です。

## コラム.6 デジタル遺産相続

近年、生活の中にIT機器やウェブサービスが深く入り込むにつれ、必要となるIDとパスワードの数は増加する一方です。

例えば家族の中でITに詳しい人が1人だったり、あるいは互いになにを利用しているか話していなかったりした場合、その方が亡くなると、資産や負債を含めて、こういったものが残されたのかわからない場合もあります。

とくに、問題になりやすいのは負の遺産で、FX(外国為替証拠金取引)で取引をしたまま亡くなった場合、取引が継続されており、その後相場が大きく変動するなどして、知らないうちに莫大な負債(不足)を抱え込んだという例もあります。逆に、暗号資産が相当額あるはずなのに引き出し方がわからない場合もあり得るでしょう。

「立つ鳥跡を濁さず」、きれいな終わり方にするためには、残された人が困らないように、万が一のときに備えて管理情報のありかを残しておきましょう。

こういったサービスを利用して、いたかの一覧や、もし亡くなったらどのような処理をしたらよいか。IDやパスワードなども、パスワード帳に書き残すか、スマホのパスワード管理アプリ▶用語集P.200を利用している場合その解除のためのPINコード▶用語集P.191などをノートや遺言書に残すなどして、残った家族が分かるようにしておきましょう。SNSのウェブサービスなどは、本人が亡くなった場合、特定の人を管理者に指定できる機能が提供されている場合もありま

### きちんと伝えておかないと、突然負の遺産が現れることも



これは極端なたとえですが、お金のやりとりが発生するサービスをそのままにしておくと、支払いや負債が残された家族にかかってくる場合があります。

### なにをやっていたかをパスワードを含めて書き残す



お金のやりとりがあるものは支払いや負債が発生する可能性があり、ブログや電子メールアカウント、デジタル写真サービスは乗っ取られる可能性があります。誰かが相続し管理をするか、運営者に死亡を伝えるなどしてきちんと終了させる必要があります。管理に必要な情報をパスワード帳などに書き残すのも1つの方法です。

す。調べてみましょう。

残された家族が美しい思い出に浸りながらあなたを偲ぶことができるようにするためには、自分が

いなくなった後も適切な処理ができるよう、デジタル遺産▶用語集P.199をきちんと整理しておくことが大切です。

## 第4章

# 災害・テロ、海外でのトラブル、 普段とは違う環境のリスクに備えよう

災害・テロなど、非常時にもインターネットにつながり情報収集することは大切です。  
また、海外でインターネットを利用する際、日本では遭遇しないトラブルやリスクがあります。  
普段とは違う環境に備えるには、普段からどんな準備をしておくとういかが学びましょう。

### 1 大災害やテロに備えよう

- 1.1 まずは自分の身の安全を確保する
  - 1.2 電池をもたす、情報収集をする
  - 1.3 ラジオ、車載テレビを使った情報収集
  - 1.4 徒歩帰宅、海外での災害やテロに備えて
- コラム.1 国により異なる情報の取扱。海外でトラブルに巻き込まれないように

### 2 屋外・海外でのインターネットの利用には注意しよう

- 2.1 一見なにもないように見えて、危険がいっぱい
  - 2.2 インターネットカフェの利用
  - 2.3 海外でスマホやタブレットを活用するために
- コラム.2 災害時の情報収集について

## 1

## 大災害やテロに備えよう

## 1.1 まずは自分の身の安全を確保する

最近では各種の自然災害やテロなどが発生すると、その状況をネットにアップする人がいます。しかし、なんらかの災害・テロの発生や避難勧告が発表されたら、写真を撮ったりSNS▶用語集 P.192 に投稿したりせず、速やかに安全な場所に避難しましょう。

海や川の近くでの大地震ならば、急いでできるだけ高い場所に避難しましょう。

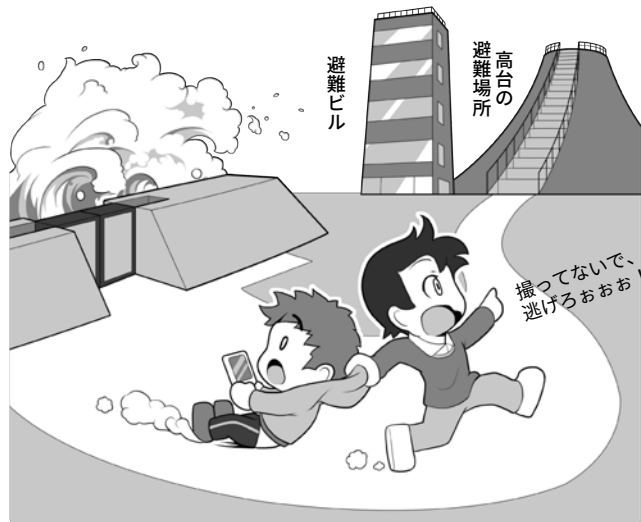
災害時に現場で写真を撮ったり、実況放送のようにレポートすることは、あなたの仕事ではありません。無事家族や同僚の元に帰ることが使命です。それを最優先に考えて、まずは命を守る行動をしましょう。

避難場所に到着し、そこが安全であると確認できたら、安否確認の連絡や情報収集をしましょう。

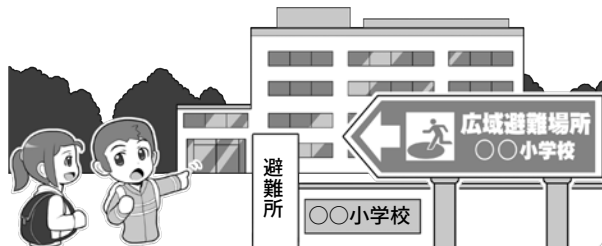
安否確認サービスはさまざまなものがあるので、事前に家族や同僚たちと、どのサービスを利用するかを決めておきましょう。また、災害時は電話やウェブサイト▶用語集 P.194 の閲覧などは混み合ってつながりにくくなります。災害時に通話が優先される公衆電話や、なるべくデータ通信量の少なくてすむ、メールやSNSのメッセージなどのサービスを使いましょう。

なお、スマホアプリの通話機能もメールなどより通信容量を多く使います。譲り合い、少ないデータ通信ですむ手段を優先しましょう。

## 命を脅かすものから速やかに逃げる



## 安否の連絡や情報収集は安全な場所に着いてから



自然災害時は避難勧告が出る前でも、自主的な避難が命を守る行動になります。まずは身の安全を確保し、その後、安否の連絡や情報確認を行いましょう。

## そして安否連絡や安否確認サービスに登録



安否確認の方法は、複数の候補を事前に家族や同僚などで決めておいて、それらを利用するようにしましょう。災害時には、スマホを含む一般の電話は通話がつながりにくくなります。電話連絡をする場合は、公衆電話か避難所に設けられる災害時用の電話を利用しましょう。なお、インターネットが使えなくなった場合の避難手順や安否確認方法も検討しておきましょう。



## 1.2 電池をもたす、情報収集をする

災害時、街中なのにスマホが圏外になったら、それは通信用の基地局が被害にあって壊れている印です。そのまま電源をオンにしておくと、スマホはつながらない基地局に接続しようとして、普段以上に貴重な電池を消耗してしまいます。

そういったときはスッとスマホの電源を切るか、スマホの中身を見る場合でもフライトモード（機内モード）▶用語集 P.202 にして少しでも電池の消費を抑えましょう。

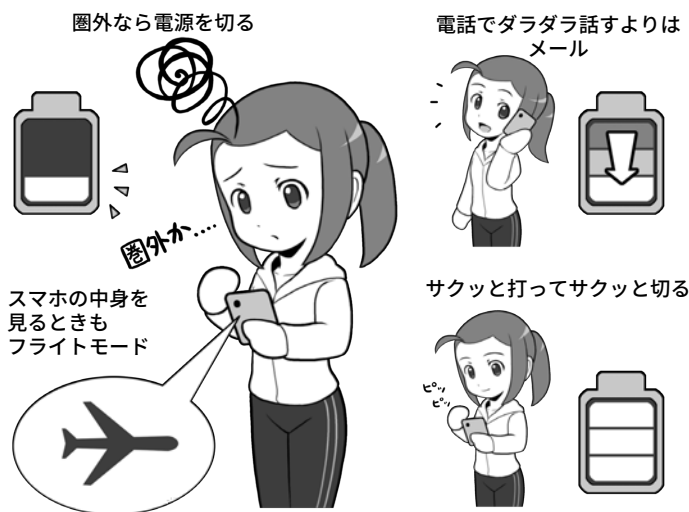
電波が回復しても、電話よりはデータ通信のメールやSNSを利用しましょう。災害時はそのほうがつながりやすく、また、電池の消費も少なくて済みます。次にいつ充電できるかわからない状況では、とにかく電池の節約を心がけるようにしましょう。いざというときに備えてACアダプター一体型のモバイルバッテリーを、日常的に持ち歩くのもよいでしょう。

災害直後は情報が錯綜しますが、一定時間が経過すると救援物資や脱出ルートなどの情報がネットに掲載され、やがて整然とした情報発信が行われるようになります。

しかし、だらだらとウェブサイト回って情報を収集しても電池を消費するだけなので、メールやSNSで、情報の収集と整理に長けた家族や親しい友人や遠隔地にいる同僚に助けを求め、信憑性や関連性の高い情報、必要としている情報だけを整理して送ってもらうのもよいでしょう。その他、災害時に利用可能になる、通信事業者が運用する伝言板システムを使い、対応に必要な情報を募る／安否確認を行うなども考えられます。

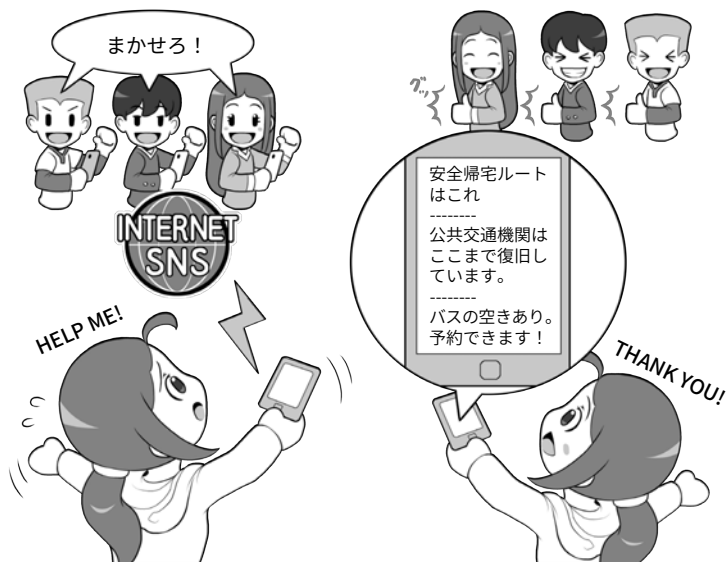
東日本大震災では旅行で被災地に

### 電池をもたすテクニック



電波が圏外ならば電源を切るか、スマホの内容の閲覧時もフライトモードを利用します。電波が回復したら災害用の超省電力モードがあれば活用してもよいでしょう。電話で長く話すよりも、メールをさくっと打って電源を切ったほうが電池を消費しません。AC コンセントがあれば充電器にもなる一体型モバイルバッテリーを持ち歩くのも役立ちます。

### 情報収集に協力してもらおう



情報収集に長けた家族や友人・同僚に相談して、いざというときは情報収集や必要な交通手段の手配をお願いできるようにしておきましょう。自分1人では気づかない情報も外から見ていると気づく場合もあります。

訪れているときに震災に遭い、帰宅できなくなった方たちが、SNSを通じて友人に被災地から家に帰るためのルートの確認や車両手配、バスの予約などをしてもらった例もありま

す。同僚たちと検討してみましょう。

ぜひそういった事例をみんなで話し合って、いざというときにどうするか、ということを相談しておいてみてください。

## 1.3 ラジオ、車載テレビを使った情報収集

大災害時に、通信用電波がきちんと飛んでいる状態でも、目的のサーバに接続しようとする、反応がない場合があります。

それは、サイバー攻撃のDDoS攻撃▶用語集 P.190のように、多くの人が特定のサーバに集中して接続することで、サーバの反応が間に合わなくなり、ギブアップの状況になっている可能性があります。

この問題は災害時には避けがたく、双方向通信のメディア、つまり私たちがサーバに接続してサーバが返信するというプロセスを前提としているインターネットでは、どうすることもできません。

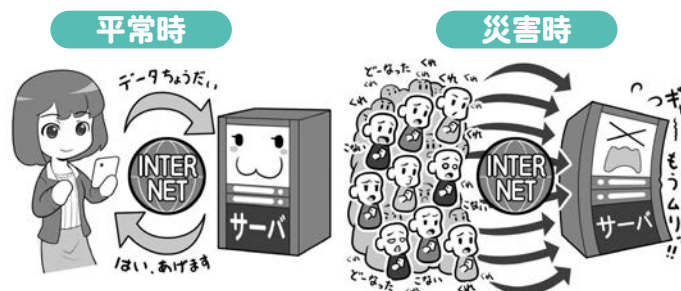
こういったときに力を発揮するのが「片方向通信メディア」である、ラジオやTVです。これらのメディアは送信局が一方向的に情報を発信して、私たちは受信するだけなので、ウェブサーバのようにアクセスが集中し反応できなくなるということはありません。

比較的近距离を放送のエリアとするテレビやFMラジオなどは、大震災時などに送信局や送信施設が自分と同じように被災して活動できなくなっている可能性があります。しかし、一局で広範囲に電波を送信できるAMラジオや短波放送ならば、災害時に放送が中断する可能性が、FMと比較して少なくなります。

これが災害用の持ち出し袋にAM放送を受信できるラジオを入れる理由でもあります。

トラブルに対しては複数の手段で備えるのが基本ですから、普段は聴くことがなくても、災害用持ち出し袋にはAMラジオを入れることを検

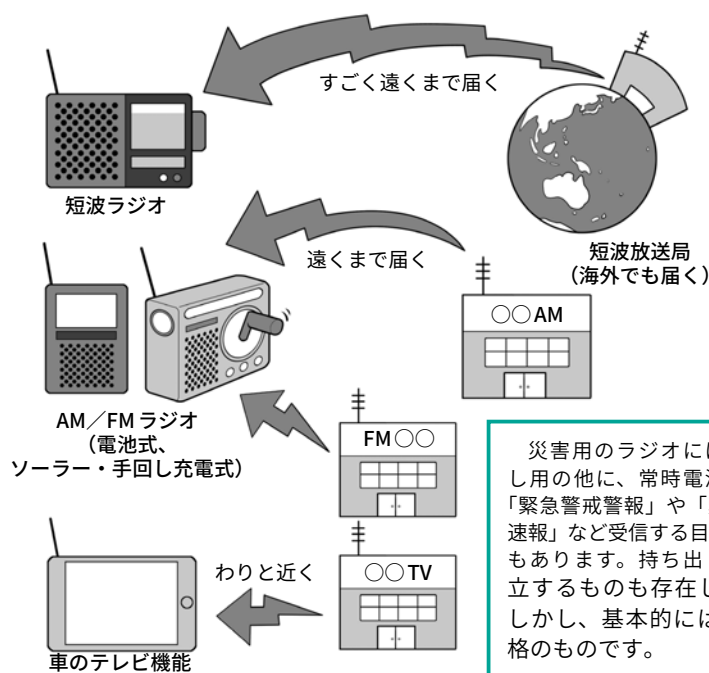
### 災害時のアクセス集中によるサーバの沈黙(双方向通信)



インターネットでは私たちのリクエストにサーバが答えることで、情報が閲覧可能になります。しかし、一気にリクエストが集中するとサーバの処理能力を超えるため、反応が返ってこなくなります。これがアクセス集中による沈黙（サーバダウン）です。

### 災害時でも沈黙しないラジオやテレビ(片方向通信)

ラジオ・TVは一方向的に送信できるので大丈夫



片方向通信の機器は、対応する受信機を持っているすべての人が受信可能です。FMやテレビは放送局も被災して発信できなくなることがありますが、AMではかなり遠くまで届くので別の地域のもを拾うことができる場合もあります。短波にいたっては海外まで届きますが、逆に地域別情報発信には不向きです。ラジオは消費電力が少なく、ソーラー充電や手回し式充電型も実用的です。通常のテレビ受信可能な車のカーナビもいざというときには頼りになるはずで

討しましょう。なお乾電池は、定期的に液漏れをチェックしましょう。

また、自分が持っていないと意外と忘れがちですが、車の中ならAM/FMのラジオ、一部は車載テレビでテレビ放送が受信できます。

車の中には、USBコンセントやACコンセントを使用可能なものもあります。自分の車がそのような車種であるならば、災害に備えて燃料を一定以上入れておき、非常用電源としても機能するようにしましょう。

## 1.4 徒歩帰宅、海外での災害やテロに備えて

災害時は原則としては政府や各自自治体・消防などの指示に従うべきですが、ときに徒歩帰宅をする選択肢を取らざるを得ない場合もあります。

スマホには学校や仕事場から自宅までの道中、災害時に役立つ情報を掲載した帰宅支援マップやアプリを入れておきましょう。日没時や降雨時の避難場所などもわかります。

その場合に備え、家族と落ち合う集合場所や、帰宅手順を話し合っておきましょう。長期大規模停電で通信できない状況まで想定して、プランを立てましょう。

災害時にはスマホの電池が命綱になる場合もあるので、普段からACアダプター一体型のモバイルバッテリーや、車の電源を活用できるようにカーチャージャー、充電用ケーブルなどを持ち歩きましょう。

海外出張や旅行時の災害やテロに備える場合は、事前に外務省の「海外安全ホームページ」で渡航先の情報を確認し、渡航が推奨されない地域には行かないようにしましょう。

また、渡航前に外務省の海外安全情報配信サービス「たびレジ」に登録し、リアルタイムで渡航先の安全状況が把握できるようにしましょう。

万が一災害が起こった場合に、緊急時の安否確認などがすみやかに行えるように、ショートメッセージ(SMS)▶用語集 P.192 を受け取れるようにしましょう。

「海外ではどういう風にデータ通信をするか」を前提に考え、とくにデータ通信しない場合でも、いざというとき、慣れない土地で身を守るためには、最低限上記のSMSメッセージは必要なんだと覚えておきましょう\*。

\* ショートメッセージ(SMS)は基本的には通常の携帯電話回線(インターネット電話ではない)を利用して、データ通信を利用していなくてもメッセージを受け取ることができます。

### 災害時に徒歩帰宅をする場合は

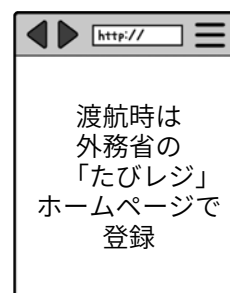
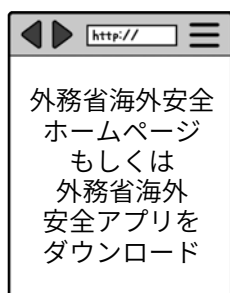
#### 帰宅マップ



災害時は、政府方針で最大3日程度現地に待機を求められる場合もあるので、スマホなどの情報機器を使う場合、電池を持たず準備が大切です。ACアダプター一体型のモバイルバッテリーの携帯や、車で充電できるようにUSB端子のついたカーチャージャーを必要に応じて携帯しましょう。また、自分の機器の充電に対応しているかもチェックしておきましょう。条件に合わないとう充電できないこともあります(主に2Aや2.1A対応と書かれている給電能力が推奨)。

### 海外での災害やテロに備える場合は

#### 渡航前後に現地の情報を確認する 外務省たびレジに登録する



緊急時は  
SMSで連絡

#### たびレジ簡易登録にメールアドレスを登録する



注)「外務省海外安全アプリ」では、約120ページの「海外安全虎の巻」が同梱されていたり、海外安全にかかわる外務省のホームページなどを簡単に分類し、手早くアクセスできるようになっていたりするので、ぜひダウンロードしておきましょう。



インターネットは国境を越えて世界の人々を繋ぎ、理想的には皆同じ基準で、平等にその恩恵を享受できるべきです。しかし、現実的にはそれぞれの国の中ではローカルルールによって、さまざまな制約を受ける場合があります。

その国のルールを理解せず、自国の常識でネットを利用すると、思わぬトラブルに遭遇することもあるので注意が必要です。

ここでは、あなたが他国に旅行やビジネスで訪れると想定して、遭遇するトラブルを、あくまでフィクションとしてですが考察してみましょう。

### ■ 1. 入国まで

あなたがA国に訪れたいと考えました。ビザは免除されていますが、テロ対策の点から、事前に入国登録することが求められました。項目には「利用しているSNSアカウントを全て記入せよ」というものがありました。

これはSNSアカウントの書き込みから、テロを起こす過激思想を持っていないかを判断するために利用するようですが、日本ではちょっとした冗談の書き込みでも、A国ではそう受け取られず、入国を拒否されそうになりました。

入国したら、今度は入国審査で、利用しているスマホやパソコンのパスワード▶用語集 P.200を開示せよと言われました。さまざまなサービスのアカウントの分もです。書き出したものの一覧を見ると、係官は鼻で笑い、ロックを外された機器は別室に持って行かれ、コ

ピーを取られました。あなたは長い間待たされたあげく、今度は取調室に呼ばれます。

そして、スマホに保存していた特殊な嗜好のマンガや写真の所持を指摘され、法律違反で逮捕され、起訴され、懲役判決を受けるかもしれないと言われました。私たちの国では問題無くても、そういったものが法律あるいは宗教的に許されない国も、世界にはあります。

また、スマホのアルバムに保存していた自分のこどもの着替え中の写真が、サーバが置かれた国のルールに従って、「児童ポルノ」と判断され、国際的に手配される可能性があるかもしれないという話もありました。

### ■ 2. 入国してから

やっとの事で入国することはできましたが、パソコンは没収されてしまいました。

スマホは戻ってきたものの初期化されていました。通信しようとしたらローミング▶用語集 P.204では著しく遅いので、値段も手頃な現地で販売しているその国の携帯電話会社のSIMカードを購入しました。代金はクレジットカードで支払います。

ところが、スマホを元の状態にリカバリしようとアプリストアを見ると、普段使い慣れているエンドツーエンド暗号化のSNSのアプリがありません。そうやらその国では、使い慣れたSNSアプリが禁止されているようです。かわりにVPN▶用語集 P.193を使おうと

したら、度々VPN機能がオフになります。やっとの事で見つけた通信暗号化するメッセージアプリをインストール▶用語集 P.194したら、今度は通信ができなくなりました。

### ■ 3. 撮影していると…

携帯電話会社のお店に駆け込んで、通信ができなくなったと思ったら、別のSIM▶用語集 P.192を買うことをすすめられました。仕方が無いので、再度購入します。

回線が復活したので観光に戻って、現地での様子でも写真で撮って送ろうと、車での移動中や観光地で撮影をし、日が暮れたのでホテルに戻りました。

夕食を終えて部屋でくつろいでいると、突然部屋に警察官が入ってきて連行されます。軍事施設を撮影した容疑で逮捕されたのです。そんな場所を撮影した記憶は全くないのですが、確かに撮影したと言われ、またしてもスマホを取り上げられました。

同行者が速やかに大使館に連絡をしてくれたので、やっとのことで数日後釈放されました。

### ■ 4. 日本の常識は通じない

取り調べの過程で所持品も色々没収されてしまったので、足りないものを翌日配達ของオンラインショップで購入します。アカウントを取得しクレジットカードを設定し、不正利用が怖いので、SMS経由でワンタイムパスワード▶用語集 P.204を入力する二要素認証を設定しました。

翌日、家族に帰国の日程を報告



するべくスマートフォンで電話しようとする、また通じなくなっていました。

仕方ないのでホテルの電話で連絡し、準備を整えてチェックアウトしようとしたら、クレジットカードも使えなくなっていました。

クレジットカード会社に問い合わせると、昨日利用したオンラインショップで、一度に多量の購入があったので、利用を停止したとのことでした。

二要素認証を設定していたのに、なんで使われてしまったか調べたところ、電話番号を乗っ取るSIMハイジャック▶用語集 P.192 という攻撃に遭っていたことが判明しました。

インターネットは世界を繋ぎますが、実状として、訪問した国のルールや物理的なサーバの所在国のルールが適用されます。

自国の慣習をそのまま持ち込んだり、よく考えずに利用したりせず、必ず調べてから利用しましょう。また、海外進出を検討している中小企業などは、進出前には必ず現地国のデータの取扱いやクラウドサーバ▶用語集 P.195 の所在地を確認しましょう。そして、重要な情報は自国にサーバのあるサービスを利用した方が無難です。

## 国によっては問題となってしまうデータの取扱い

### ① 自国で問題ない写真がアウトなことも



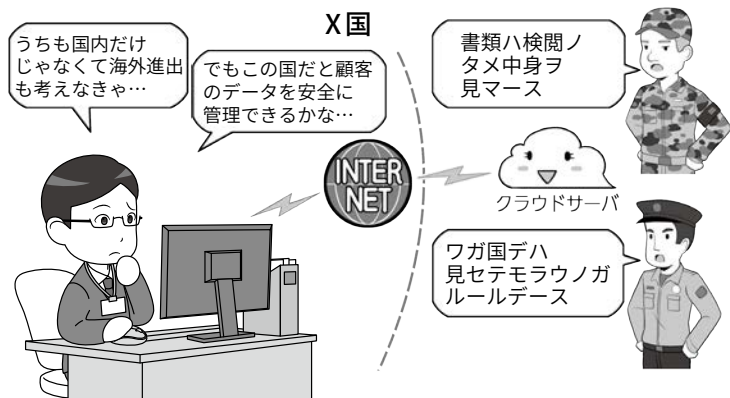
我が国の常識がそのまま外国の常識や法、宗教的規範に合致するとは限りません。そのルールに反すると、最悪の場合実刑を受けることもあります。

### ② 他国ではどこでも撮影してよいとは限らない



また、軍事的にセンシティブな国では、関連施設にカメラを向けるだけで、スパイ▶用語集 P.197 容疑をかけられて拘束されることもあります。ルールを調べてから渡航しましょう。

### ③ クラウドサーバのデータは所在地の国のルールに従う



クラウドサーバにあるデータは、サーバの実際の所在地や提供する企業の法に従って、その内容が検閲され、その結果情報が流出する可能性もあります。要注意です。

# 屋外・海外でのインターネットの 利用には注意しよう

## 2.1 一見なにもないように見えて、危険がいっぱい

つぎにお店が開放しているアクセスポイントがしっかりとセキュリティ対策されているかも確認すべきです。お店の無線LANアクセスポイントの暗号化▶用語集 P.194 は本当に安全な方式か？攻撃者▶用語集 P.196 がお店のアクセスポイントと全く同じ名前の偽のアクセスポイントを設置してあなたを待ち構えていないか？利用時には注意が必要です。またあなたが通信しようとする先がHTTPS (P.130 参照) など暗号化通信を行うようになっているか、もしくは使う

総務省が無線 LAN (Wi-Fi) ▶用語集

P.203を安全に利用するための簡易マニュアルを公開しているので、参考にしましょう。

## 2.2 インターネットカフェの利用

海外旅行に出かけるときになるべく荷物を減らそうとすると、仕事での渡航でないなら、パソコンはお留守番になるでしょう。

最近では、スマホもありますし、長いメールを書く必要があるなら、インターネットカフェに行って、ウェブメールを利用すれば、ホテルでもなんでも予約できるし…、なんて思っていないですか？

インターネットカフェは、国内外を問わず便利ではありますが、これを使ってメールやなんらかのウェブサービスのID・用語集 P.191 とパスワードの入力、あるいはクレジットカード情報の入力は、絶対に避けることをおすすめします。

海外のインターネットカフェのパソコンは、管理が充分ではないことがある他、攻撃者にとっても狙いやすいターゲットでもあります。キーロガーというマルウェアを仕込んで、利用者が入力したIDやパスワードなどの個人情報を抜き取って攻撃者に送信してしまうことがあるのです。

お店の人がシステムを最新に保ち、セキュリティソフトも入れ管理しているから、そんなソフト仕込めないよ、と思ったら甘いのです。キーロガーにはハードウェア版もあり、数秒あればパソコンの本体の後ろ、キーボードのUSB端子と本体の間に装着でき、あとは無線LAN経由でデータを送信できるものもあります。今まで利用したパソコンの後ろをいちいち確認したことはないでしょう？

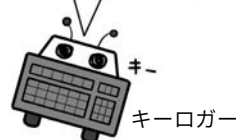
また、自分のパソコンやタブレットを持ち込んで店のWi-Fiを

### インターネットカフェのマシンには、キーロガーなどが仕込んである前提で利用する

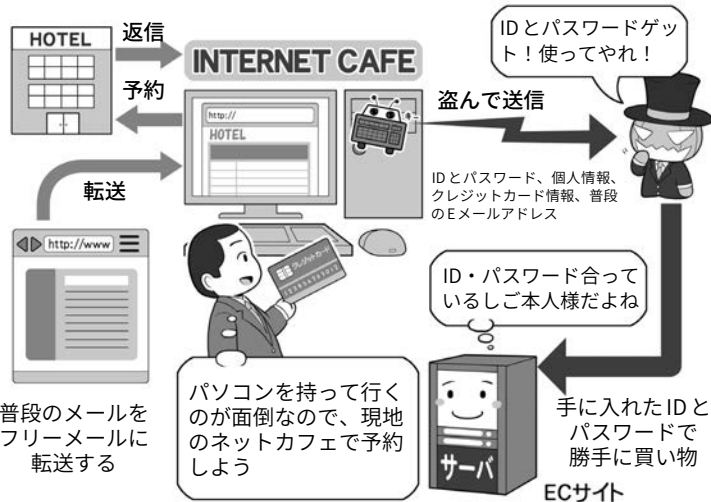


インターネットカフェは、基本的に情報を検索するだけに利用します。IDとパスワード、個人情報、クレジットカード情報は絶対に入力しないように。自分の持ち込みパソコンなどを利用する場合は、自前の通信の暗号化ができるならOKです。

キー入力を横取りして勝手に使っちゃうぞ！



### 共用のパソコンで重要な情報をやりとりしたら攻撃者に漏れる可能性あり



### データローミング

現地で頻繁に個人情報などを入れてやりとりする必要があるならば、データローミングの端末で操作する

インターネットカフェで普段利用しているウェブメールを使うのは危ないと考え、フリーメールアドレスを作成しそこにメールを転送しても、結局予約のやりとりなどを現地で行うことになるのなら、情報流出の危険性はわかりません。

現地でそういった情報を入力することが多いのならば、タブレットなどでデータローミングを行うか、自前の暗号化+公衆無線LANを使うようにしましょう。

使用する場合は、自前の暗号化ができないなら利用はおすすめしません。もし現地で頻繁にデータ通信を利用するならば、データロー

ミング▶用語集 P.199 や現地の定額SIM(次頁参照)の使用をおすすめします。



## 2.3 海外でスマホやタブレットを活用するために

スマホやタブレットを海外出張や旅行に持って行き現地で使う場合、日本で契約している携帯電話会社が提供するローミングサービスを使って、現地の携帯電話回線提供会社と契約を交わさないまま、データ通信を利用する方法があります。

ローミングサービスは国内よりは割高で、音声とデータ通信は別々に料金設定されていることもあるので、利用したらいくらかの金をよく確かめておきましょう。さもないと払い切れない料金請求が届く場合があります。最近は手頃な1日あたり料金定額などのプランも存在します。

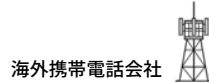
また、海外では電話を受けただけでも電話料金がかかる会社もあります。着信が無料ではない場合、電話を受けたらいくらかかるのかもチェックしておきましょう。さもないと、不意の長話で高額な請求が来てしまうかもしれません。

データ通信が使えなくも文章のやりとりをする方法にショートメッセージ(SMS)がありますが、これも利用可能かどうかと、利用できる場合の料金を調べておきましょう。電波整備状況が悪くデータ通信が使えない場合の、貴重な文字通信手段になります。

ローミングサービスを電話で利用するメリットは、海外にいても(高額ですが)自分の電話番号にかかってきた通話を受けられることです。

もし長期で滞在する場合などで、その間電話番号が変わってもよいならば、現地携帯電話会社のSIMを購入して利用する方法もあります。SIMには目的別に音声のみ、音声＋データ通信、タブレット用にデータ

### 海外で電話やデータ通信を使う



普段の電話番号で着信できるようにする

電話番号が現地のものになってもよい



音声利用：  
マイ端末で(音声)  
ローミング



データ通信利用：  
マイ端末で  
データローミング



音声利用：海外はSIMフリー  
相当のマイ端末か、SIM  
端末と現地SIM



データ通信利用：海外はSIM  
フリー相当のマイ端末か、SIM  
フリー端末と現地SIM

現地SIMは現地空港  
などでも買えるが……



- ・日本で買えることも(SIMのサイズに注意)
- ・事前使用設定を済ませておく
- ・音声の料金、データ通信の上限容量をチェック
- ・月額料金が発生せず、チャージすれば保存可能なものもある。何回も訪れるなら選択肢に
- ・料金は従量制か、上限のある定額制か確かめる

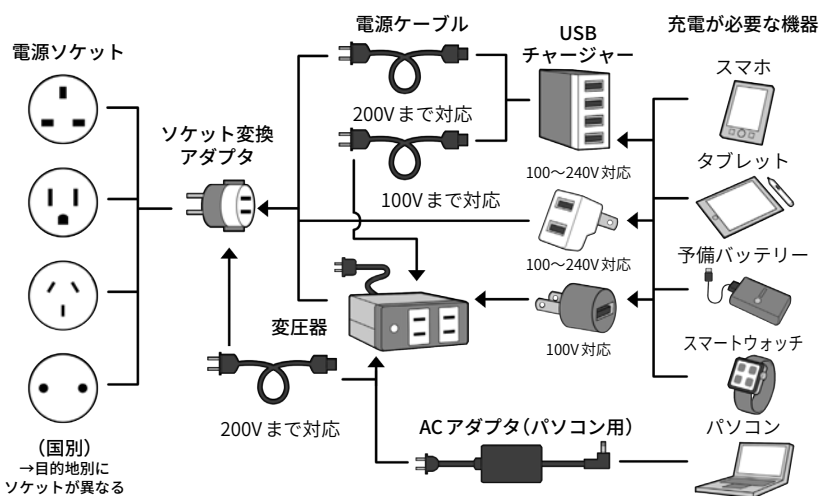
外国語が苦手だからメールで  
やりとりしようと思ったら



海外では意外とデータ通信できず、音声のみのエリアも多いのです。データ通信できても遅い場合もあります。データ通信速度を確保できないことを想定して、地図アプリの地図データなどは日本で事前にダウンロードしておくことを推奨します。

### 電源・充電方法の確保

ソケットと電源のボルト数はまちまち。  
理想的にはすべて100～240V対応であること



USB充電器▶用語集 P.193 のUSB端子は、充電する機器の数だけ差し込み口はあるか、全体の電源容量は足りているか、タブレット用には充電能力は足りしているかチェック。200V系の国へ訪問するときは、ケーブルまでもが200V対応かを確認します。



通信のみなどのSIMが存在します。

普段の端末は日本からの着信専用にして、別途SIMフリー▶用語集 P.192の端末を用意し、これに現地のSIMを入れて使用する方法もあります。

海外のSIMを使う場合の注意点は、利用する端末が「SIMフリー」であるか確認することです。2021年8月に総務省が改正した「移動端末設備の円滑な流通・利用の確保に関するガイドライン」(通称：SIMロックガイドライン)によって、2021年10月以降、国内で販売される端末は、販売元の会社以外のSIMを使用できないようにするSIMロックが禁止となったため、SIMロック解除の手続きは原則必要ありません。しかし、それ以前に販売された端末ではSIMロック解除が必要になる場合もあるので、使用している携帯キャリアの情報を確認しましょう。

忘れがちなのが充電に関することです。充電器の対応電圧と、充電器にケーブルがある場合はこのケーブルの対応電圧が訪問国の電気事情にあっているか確認して、必要に応じ変圧器を利用し、現地のさまざまなタイプの電源ソケットの形状に対応できるソケット変換アダプターを用意しておきましょう。

次に、せっかくスマホなどを海外に持っていくのなら、海外で使えるアプリや役立つアプリを準備していきましょう。

まずは翻訳系です。文字を入力するのではなく、音声で入力、翻訳結果も音読してくれるアプリなどもあります。また逆に相手にしゃべってもらってそれを翻訳することもできるので、音声を使って現地の人と理解を深め合うことができます。

次は翻訳カメラ。海外で街並みやメニューなどを撮影すると、文字部

## 海外でITを活用する

### 翻訳アプリ



### 翻訳カメラ



### 地図ソフト、GPSナビ



### (音声)ローミングの注意点



- ・海外では通話を受けても料金がかかる場合もある
- ・ローミング時の料金はいくらかかるのかチェックしておく
- ・ショートメッセージ(SMS)が利用できるかどうかと、その料金

### データローミングの注意点



- ・必要がないなら、データローミングの設定を必ず切る
- ・つながるからと放置しておくと、莫大な請求金額がくる場合がある

## 海外利用におけるSIMフリーとは

### 手持ちのスマホなどが海外でも使えるか



- ・目的の国でのローミングに対応しているか、実際に使用されているか。現地の会社の周波数帯(バンド)に合っているか
- ・海外のSIMが使用可能か(≒SIMフリー)

### 日常使っているスマホなどを、SIMを入れ替えて使う



- 現地SIMなら料金も手頃なものがあり、電話料金も安い
- ✗ 日本から普段の番号に電話できない。滞在期間中の電話番号を覚えておく必要あり

### SIMフリー端末の入手とは



- ・日本では特定の会社のSIMのみ利用可能だが、海外ではどれでもOK(海外では「SIMフリー」相当)
- ・お金を払うと携帯電話会社がSIMフリー状態に改修してくれる(SIMフリー)
- ・そもそも電気店やメーカーから直接SIMフリーのスマホを買う(SIMフリー)

### 普段使っていないSIMフリー機を使う



- 手頃なSIMフリー機を入手するか、使わなくなったものをSIMフリー化しておく  
現地SIM使用、料金も手頃
- 普段使用の機種は電話を受けるだけのローミング。日本の電話番号でかけられる
- ✗ 2台持ちは面倒

分を認識し翻訳して表示するものです。こちらもいちいち辞書アプリなどに文字を入力する手間が省けますので、海外の旅をより楽しむことができるでしょう。

地図系のアプリのインストールと、現地の地図のダウンロードも重要です。前述のコラムでも書きましたが、海外では場所によっては日本のよう

に通信網が充実しておらず、データ通信があっても遅いか、場所によっては全く使えないこともしばしばです。そんな中で現在地を確認しなければならない状態になったとき、オフラインでも使えるように、該当の地域の地図データを、あらかじめスマホ本体にダウンロードしておけるものを準備して行きましょう。

## コラム.2 災害時の情報収集について

近年は、さまざまな自然災害が発生し、その中でさまざまなデマが飛び交い、正確な情報収集の難しさを浮き彫りにしました。悪意のデマではないとしても、不正確な情報の拡散も多く見受けられました。拡散する方々は善意で行っているのですが、情報源(ソース)がはっきりしないものの拡散は状況を混乱させます。物事の正確さを担保するためには、「現場」を知る責任がある方の「公式な情報発信」以外は、むやみに拡散するべきではありません。とくに、「誰かに聞いた」という伝聞は、たとえそれが「通信会社の人に聞いた」「役所の方が言っていた」というものでも、公式発表ではないかぎり、「不正確」である可能性が高くなります。「伝聞情報」には気をつけて、「本当に拡散するべきか」よく考えてください。昨今は、耳目を引きやすいフェイク画像を簡単に生成できるウェブサービスもあり、SNSで流布している画像がフェイクである可能性もあります。公式もしくは信頼できるメディアからの情報でない限り留意しましょう。公開した情報が「悪質なデマ」と認定されると、公開した当人が何らかの罪に問われる可能性もあります。

また、災害時の救助要請をSNSで行う方法が、広く一般に認識されたことが確認されました。これも本人、もしくは直接依頼された家族などの代理人が行うことは大変有効な手段ともいえますが、上記と同様に伝聞の情報を拡散したり、あるいは本人が救助された後も救助要請が残されたままだっ

### 災害時の救助関係発信はわかりやすく確実に



公的機関の災害時の窓口は、あくまでも 110 番 119 番の電話ですが、SNS で救助関係の発信をするときは、住所や GPS 情報を付けましょう。

たりすると、それが1人でも多く助けようとする方の妨げにもなります。それ以外にも SNS の情報を見て、直接関係がない人が善意で電話での救助要請を行うなどのケースがあったようです。

こういった情報は、本当に必要な情報収集への「雑音(ノイズ)」となる可能性があるので控えましょう。

また、最近はさまざまな災害時のアプリが登場し、安否確認の方法も増えてきていますが、これらは連絡を取り合う人と、事前になにを使うか決めておかなければ意味を成しません。きちんと利用するサービスの確認をしておきましょう。

なお、2018年に北海道を襲っ

た地震では、全道が長期間にわたって停電する事態が発生しました。携帯電話網もスマホも使えなくなる可能性が垣間見えた災害でした。そういった場合どういう手段で連絡を取り合うかも確認しておきましょう。

災害時の避難所などでは、自治体や電気通信事業者の取組により、無料で使える Wi-Fi「00000 JAPAN▶用語集 P.190」などが立ち上がることがありますが、この Wi-Fi は接続しやすさを優先するため、暗号化されていないことを覚えておき、利用時は ID とパスワードの入力を避け、もし利用したい場合は VPN など自前で通信を暗号化する知識を得ておきましょう。

## 第5章

# スマホやパソコン、IoT 機器を 安全に利用するための設定を知ろう

スマホ・パソコンを中心に、安全を守るための設定について学びましょう。またIoT 機器ならではの注意したいリスクについても解説します。どのように情報を守るか、どのように安全にインターネットを利用するか、具体的な設定方法を学び不安なく利用できるようにしましょう。

### 1 スマホのセキュリティ設定を知ろう

- 1.1 スマホにはロックをかけ、席に置いて離れたり、人に貸したりするのは×
- 1.2 不安な人は携帯キャリアのセキュリティ対策プランを検討しよう
- 1.3 総務省によるシニア向けスマホ活用支援事業を活用しよう
- 1.4 情報漏えいを防ぐ
- 1.5 スムーズな機種変更と、予期せぬデータ流出の防ぎ方

### 2 パソコンのセキュリティ設定を知ろう

- 2.1 パソコンを買ったら初期設定などを確実に
- 2.2 暗号化機能などでセキュリティレベルを高める
- 2.3 マルウェア感染に備え、3-2-1のバックアップ体制を整える
- 2.4 売却や廃棄するときはデータを消去する
- 2.5 紛失・盗難のとき、スマホとパソコン、どちらが安全？

コラム1 ダブルラインでトラブルに備える

### 3 IoT 機器のセキュリティ設定を知ろう

- 3.1 常にインターネットに接続するIoT 機器は注意が必要
- 3.2 購入後は初期パスワード変更などの設定を

### 4 それでも攻撃を受けてしまったときの兆候と対処を知ろう

コラム2 軍事スパイ、産業スパイに狙われてしまったら

## 1

# スマホのセキュリティ設定を知ろう

## 1.1 スマホにはロックをかけ、席に置いて離れたり、人に貸したりするのは×

P.40でも解説しましたが、重要なことなので繰り返します。スマホには必ずロック▶用語集 P.204 をかけてください。

ロックにもPINコード▶用語集 P.191 によるロック、パターンロック▶用語集 P.201、指紋や顔など生体情報を用いた認証によるロックなどがあります。過信は禁物ですが、生体認証▶用語集 P.198 は周りから覗かれPINコードを盗まれる危険性の排除をしつつ、入力の手間を省くので便利な機能です。

そしてセキュリティ向上のためのロック機能を設定しても、そのスマホをロック解除したまま置いてその場所を離れたり、ロックを解除して他人に見せたり貸したりすれば、せっかく施したセキュリティ対策が台無しになります。他人の手に渡れば、情報を盗まれ、乗っ取られる危険性が上がります。

スマホは大事な情報が詰まった貴重品、肌身離さず自分のそばに置き、使わないときはこまめにロックをかけましょう。

また、スマホだけでなくアプリ▶用語集 P.194 にもロック機能があれば積極的に設定しましょう。安全性を高めるには、スマホとは別のPINコード、または別のロック機能を選ぶとよいです。

しかし、ロックを設定しているからといって十分ではありません。

ロック中の待ち受け画面に表示さ

### スマホには必ず画面ロックをかけよう



本来は、上記の例のようにスマホを手放してはいけません。しかし、ロックをかけておけば、最低限のセキュリティは保てます。普段からスマホには必ずロックをかけて、肌身離さず持っておきましょう。

### 待ち受け画面の通知にはなるべく重要な情報は表示させないようにしよう



上記の例のように「こんな場所だし、大丈夫だろう」と油断してはいけません。待ち受け画面の通知は覗き見のリスクが高いため、重要な情報は表示されないようにしたほうがよいです。

れる通知内容にも気を配りましょう。とくに、待ち受け画面でメールの内容を表示できる設定にしていると、メールアドレスによる多要素認証▶用語集 P.198 を設定している場合、パス

ワード▶用語集 P.200 が記載されたメールの内容が待ち受け画面で確認でき盗み見られてしまう可能性があります。待ち受け画面に表示する通知はよく検討すべきでしょう。



## 1.2 不安な人は携帯キャリアのセキュリティ対策プランを検討しよう

スマホもパソコンと同様にコンピュータの一種です。パソコンがマルウェアの脅威、ワンクリック詐欺やフィッシング詐欺メールなどへ対策する必要があるのと同様に、スマホにもセキュリティ対策は必須です。

まず、アプリは必ず公式サイトからダウンロードしましょう。その他にも、迷惑メールを受信しないようフィルタリングや受信拒否を設定する、不用意にメールやLINEなどのメッセージ内のリンクをクリックしない、といった対策をすれば、ある程度のセキュリティは確保できますが、個人での対策は相応の知識が求められます。自ら調べてスマホの設定を確認・変更する必要があるため、スマホを安全に使えるか、正直不安を感じる方も少なくないでしょう。とくにシニアには「今年になってはじめてスマホに買い換えた」という人も珍しくなく、慣れないスマホの使い方に不安を覚えても無理はありません。またシニア本人がスマホの使用に抵抗を感じていない場合でも、遠方に暮らす高齢の家族が安全にス

**必要性を感じるなら、スマホのセキュリティ対策プラン▶用語集P.198を検討しよう**

携帯キャリア

- ウイルスメールチェック
- 迷惑メールブロック
- 危険なウェブサイトブロック
- 個人情報流出チェック
- 不正アプリスキャン

月額制で提供

プロバイダ

総合セキュリティパッケージ

上記のようなサービスをまとめて複数台に月額制で提供

携帯キャリアからは、セキュリティ関係の機能がパッケージ化されて提供され、インターネットプロバイダも、同様のサービスを提供しています。自分が求める機能があるかを精査して、必要性を感じる場合は導入を検討しましょう。

マホを使用できているか、心配になる人もいるでしょう。

現代において、スマホは、仕事や生活のあらゆる場面で使用を求められる生活必需品。もはやスマホの使用を避けることは難しいのが実状です。セキュリティ対策が心配な人は、携帯キャリアやプロバイダ▶用語

集P.202が提供しているスマホのセキュリティ対策を一括して行うプランを利用しましょう。月額で少額から利用でき、電話窓口や店頭問い合わせができるものも多いので、セキュリティ対策に不安を感じる人には心強いサービスです。

## 1.3 総務省によるシニア向けスマホ活用支援事業を活用しよう

総務省「デジタル活用支援推進事業」では、シニアなどのデジタル活用の不安解消を目的として、スマホを経由したオンライン行政手続などに対する助言・相談などを行うデジタル活用支援の講習会を実施しています。ポータルサイトにおいて動画教材なども展開されているので、積極的に利用しましょう。

### 総務省「デジタル活用支援推進事業」

<https://www.digi-katsu.go.jp/>

デジタル活用支援推進事業では、全国で講習会を開催しており会場を検索できます。また、公開されている教材・動画では、電源の入れ方、ボタン操作、アプリのインストール方法、SNSの利用方法など、基本的なスマホ操作についてわかりやすく解説しています。

## 1.4 情報漏えいを防ぐ

直接スマホを盗まれる以外の情報漏えいには、攻撃者による無線 LAN ▶用語集 P.203 を使った盗聴があります。スマホから無線 LAN のアクセスポイントの間の情報通信を盗聴するものです。これを防ぐには通信内容の暗号化▶用語集 P.194 が重要です。

P.124 からの無線 LAN の暗号化のセクションで詳しく説明しますが無線 LAN 利用時に注意すべき点は、

1. 無線 LAN 通信が暗号化されていて、かつその暗号化方式▶用語集 P.194 が安全であるか。
2. きちんと暗号化されていても、その通信で利用する「暗号キー」▶用語集 P.194 が他人に漏れていたか、共有になっていないか。
3. 無線 LAN 通信暗号化の確認だけでなく、正しい URL であることを確認し、HTTPS 通信でエラーなく接続できているかどうか。

※ 参考：総務省「WiFi 利用者向け簡易マニュアル」[https://www.soumu.go.jp/main\\_content/000690266.pdf](https://www.soumu.go.jp/main_content/000690266.pdf)

などがあります。

無線 LAN 通信が暗号化されていないまま通信をした場合、通信内容を盗聴され、ID・パスワードを盗用されて使われる、なりすましなどの被害にあう危険性があります。

次に、業務中に万が一、スマホを落としてしまった場合に、情報を流出させない方法も考えましょう。

まずはスマホの中身が暗号化されているかチェックします。古い機種では初期状態で暗号化されていないことがあります。本体と記録メディアいずれも暗号化して、落としてし

### 屋外ではむやみに公衆無線 LAN を使用しない

携帯電話会社の LTE

暗号化 HTTPS 暗号化

「暗号キー」を他人と共用しない公衆無線 LAN ※1

「暗号キー」を他人と共用する公衆無線 LAN ※2

暗号化方式が安全でない、もしくは暗号化されていない公衆無線 LAN ※3

HTTPS 暗号化

暗号化無し HTTP

そもそも自分と「契約関係がない」ものは基本的に使わず、また、運営主体がわからない無線 LAN アクセスポイントは絶対に使用しないようにしましょう。

※1 携帯電話会社やプロバイダが提供していても、「暗号キー」が共用でないとは限りません。きちんとチェックしましょう。

※2 暗号キーが貼り出してあるような公衆無線 LAN は、「暗号キー」が他人と共有になり危険です。使わないようにしましょう。

※3 無線 LAN 通信暗号化の確認だけでなく、正しい URL に HTTPS 通信でエラーなく接続できているか確認しましょう。確認を怠り、安易に ID・パスワードを入力すると盗難されるリスクがあります。

無線 LAN 暗号化などに関するより詳しい説明は、P.124 からを参照して下さい。

### 盗難されたときのために中を見られないように暗号化しよう

中のデータを見てやろう

暗号化されていて見られない！

Micro SD

本体もメディアも暗号化。最近では暗号化が標準のものがほとんどですが、必ず確認しましょう。

まっても簡単には利用できないようにしましょう。暗号化は本体のロックとセットとなり、必然的にロック機能もオンにする必要があります。

スマホを落としてしまったときの対策のためには、リモートロック▶用語集 P.203、位置情報確認やリモートワイプ▶用語集 P.203 機能を使える状態にし

ましょう。

iOS では iCloud の「iPhone を探す」、Android では「スマートフォンを探す」▶用語集 P.197」として、それぞれ該当の機能があり、パソコンや同じアカウントを紐付けた他のスマホやタブレットから操作ができるようになっています。無料なので必ず試してマスターしておきましょう。

リモートロックとは遠隔操作でスマホをロックして使えなくする機能です。スマホの所在がわからなくなったら不正利用されないよう、なによりもまずスマホをロックしましょう。

次に「位置情報」を確認しましょう。事前にこの機能を使ってスマホの位置確認ができるかどうかを試し、確実に使えるように設定しておきましょう。ただし、こども、職員や会員の監視目的では絶対に使わないようにしましょう。それはプライバシーの侵害になります。この機能は、建物の中などでは明確な場所が特定できない場合もありますが、現在のスマホのおおよそのあたりが地図上に表示されます。

見つかった場所が、自分が訪れた場所や、遺失物として届けられた警察などなら、連絡をして取り戻す段取りをします。

一方、取り戻せそうになく、とくに仕事上の問題がある場合は、最後の手段として情報漏えい防止のために「リモートワイプ」機能でスマホの中身を全部消すことも考えましょう。ただし、リモートワイプをすると、位置情報を取るができなくなりますので、情報を守るための捨て身の手段になります。

そして、仮にスマホが戻ってこな

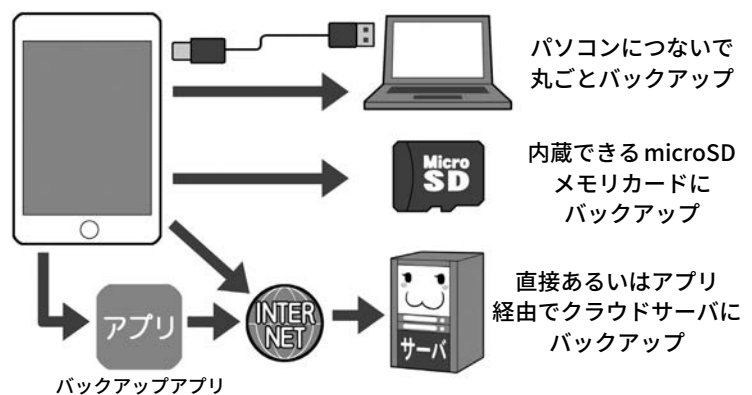
## 紛失・盗難時のために準備をしておこう



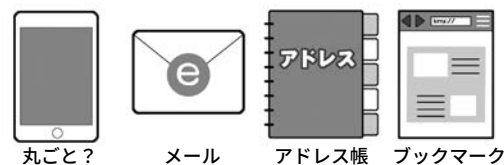
リモートワイプすると位置情報が確認できなくなるので、リスクが少ないならばロックだけ行い、遺失物として警察に相談するなどの手段をとみましょう。

## バックアップは定期的にとろう

### バックアップの方法はいろいろ



### なにがバックアップできるか確かめる



なにがバックアップできるのか確かめて、機種やバックアップ方法を選択します。

くても、本体を買い直したらすぐに復旧できるように、スマホの中身を定期的にバックアップ▶用語集 P.201 しておきましょう。機種によってはパソ

コンでバックアップすると、新しいスマホをつないでボタン一発指示するだけで復元できるものもあるので、機種選定時に調べておきましょう。

## 1.5 スムーズな機種変更と、予期せぬデータ流出の防ぎ方

スムーズな機種変更を行うためには、その前に機種変更手順を調べておくことが重要になります。

機種変更にはバックアップが重要ですが、「丸ごとバックアップ」「データごとにバックアップ」「アプリを使用してバックアップ」などさまざまな方式があります。このあたりは自分で調べるとともに、実際に機種変更やデータの移行▶用語集 P.199 をしたことがある人に聞いたり、記事を見たりして、どの方法が便利か、アドバイスを求めるなど、検討するとよいでしょう。

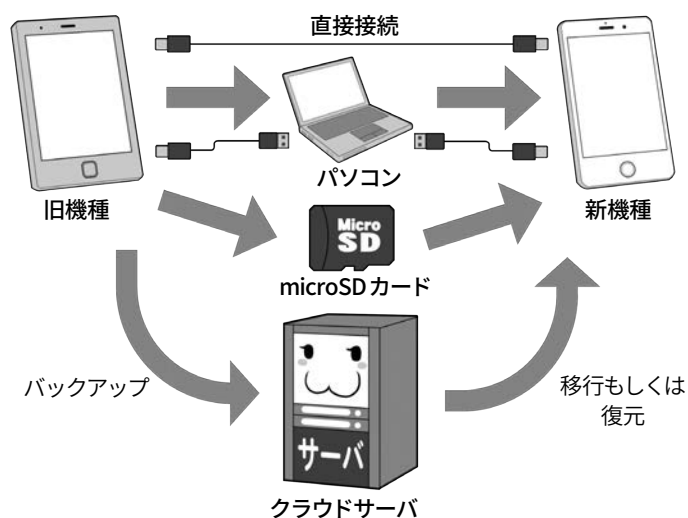
最近ではデータがスマホ自体の中（ローカル）にあるだけでなく、インターネットのどこか、利用者から見て姿が見えない雲のような存在のクラウドサーバ▶用語集 P.195 に保存されている場合もあり、機種によっては移行のためのバックアップ作業という概念そのものがないこともあります。

一方で、本体のデータ移行手段とは別に、機種変更に際して、特定の機能の移行処理をしておかなければならないものもあります。

ここ2,3年で普及したスマホの決済サービス（Apple Pay、Google Pay、おサイフケータイなど）の中には、登録しているクレジットカードや交通系ICカードなどの情報を、一旦サーバ側にバックアップしてから、かわりにパスワードを受け取り、スマホから機能を削除して、その後新しい機種でログイン▶用語集 P.204 し、そのパスワードを使い機能を復元する処理が必要になるものもあります。

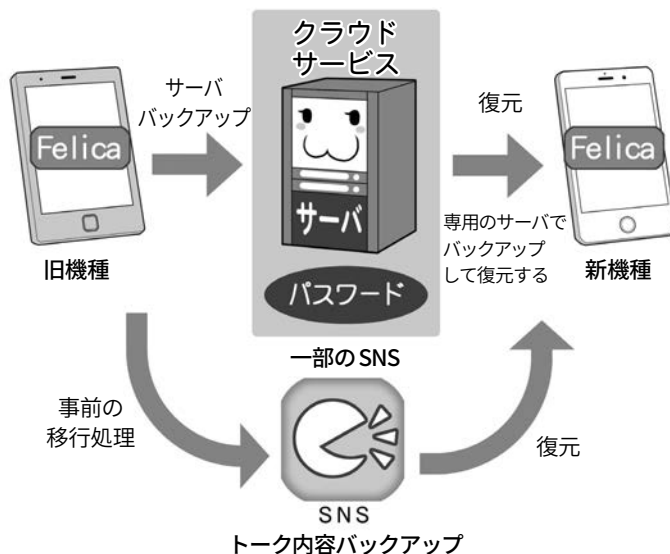
一部のSNS▶用語集 P.192 では、旧機種がアクセス可能なまま新機種から

### データの移行は事前に手段を調べる



移行処理は事前に目的の機種でこういった移行手段が使えるのか調べておきます。

### スマホの決済サービスやSNS データなどの移行



のアクセスが有効になって、同時に複数台からアクセスできてしまうようにならないように、移行処理の前に一度手続きを踏んで、旧機種からアクセス権を削除したのち、新しい機種でアクセスするための利用開始の手続きをする方式のものもあり、手間がかかります。

しかし、機種変更に伴う手続きは、

多くのサービスにおいてアップデート▶用語集 P.194 によってしばしば変更されます。

いずれの場合も機種変更の移行処理にあたって、移さなければならない機能やアプリを書き出し、それぞれの移行手順がどうなっているか調べ、各サービスを提供する企業の公式ページなど確認してください。



次は機種変更をした後の情報漏えいを防ぐ処理です。

機種変更した前のスマホには個人情報である住所録、撮りためた写真、今までやりとりしたメールなど、あなたや会社の情報が全部詰まったままになっています。売却、譲渡や廃棄する場合、必ずデータを消去しなければなりません。さもないと、知られたくないメールや写真が流出したり、住所録にある取引先に詐欺メールが送られてくるかもしれません。

また、修理に出す場合でも、モラルの低い修理会社が、芸能人のスマホから写真を抜き出して流出させた例があるので、必ずデータをすべてバックアップをした上で、本体のデータは消去してから修理に出したほうが安全でしょう。

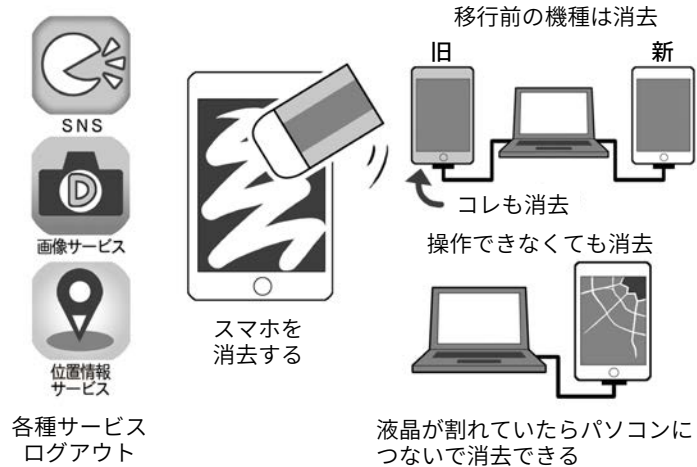
手順としてはデータをバックアップした上で、各種サービスはアプリもウェブ版もすべてログアウト▶用語集 P.204 します。続いてそれぞれのスマホにある「初期化▶用語集 P.197」や「データ消去機能▶用語集 P.199」を使って内部のデータを消去します。

一部のスマホでは、紛失時に探せるように設定した「位置情報を確認するためのサービス」を事前にログアウトしておかないと修理などに出せないものもあるので、消去の前にログアウトを確認してください。

落としてしまって液晶が割れ操作ができない場合、消去作業をすることもできないと思いますが、パソコンに接続することで消去することが可能ですので、あきらめず必ず行いましょう。

業務用に使っているスマホなどで、万が一にでもデータが復元され

## 転売、譲渡、廃棄のときは必ずデータを消去する

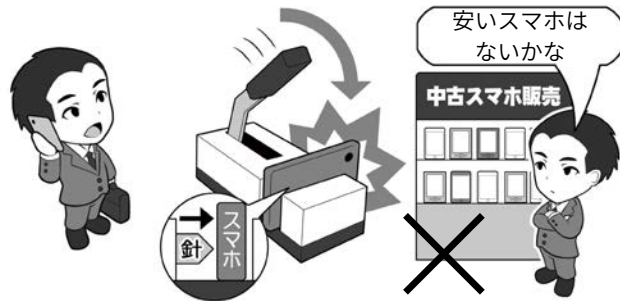


消去する前には、利用しているサービスはすべてログアウトして、サーバなどに情報を預けなければならないもの（おサイフケータイなど）は預けましょう。

SNS で移行前手続が必要なものは行い、その後移行処理をして、移行後きちんと復元できたら、旧機種を売却・譲渡や廃棄する場合は、必ずデータを消去しましょう。

液晶が割れて操作できなくても、パソコンに繋がれば消去することは可能です。一部機種ではマウスを接続して操作することも可能です。

## 業務用のスマホは物理的に破壊する。心配ならば新品を購入し、スパイウェア混入の可能性を排除する



仕事に使うスマホを廃棄する場合は、物理的に破壊する機械がある場所に持ち込んで破壊しましょう。大手携帯電話会社での回収も信頼できます。

一方、中古で購入したスマホに攻撃者がスパイウェアを仕込んでいて、企業の情報が流出しても、販売した会社にその責任を取る能力はないでしょう。ましてやオークションでの購入などではなおさらです。前所有者の残債で購入後使用不能になるケースもあります。業務用に使用するなら IT 機器は新品を利用しましょう。

る可能性を排除したい場合は、各携帯電話会社や家電量販店などで、スマホを物理的に破壊してくれるサービスを利用して、データを読み出せないようにしてしまいましょう。

なお、余談ですが、業務用などで情報漏えいのリスクを少しでも排除したいなら、中古品を購入したりし

ないようにしましょう。中古販売店が良心的でも、入荷以前にプロの組織が仕込むようなマルウェアやバックドアには対処できない可能性があります。それを避けるためには正規販売店の新品を購入して使いましょう。

# パソコンのセキュリティ設定を知ろう

## 2.1 パソコンを買ったら初期設定などを確実に

パソコンを購入したら、まず復旧のときに行うリカバリの方法を確認し、必要があればリカバリメディア▶用語集 P.203を作成しておきましょう。

リカバリメディアがDVDなどで付属している場合は必要ありませんが、最近の機種ではコストダウンの影響で添付されないものや、そもそもDVDドライブなどを搭載していないものも多いので、マニュアルなどにしたがってDVD-RディスクやUSBメモリで作成します。

なお、Windowsではリカバリメディアなどを使ったときに「プロダクトキー」▶用語集 P.202の入力が必要になる場合があります。プロダクトキーは本体の裏側や付属しているリカバリメディアにシールが貼り付けられているので、紛失に備えスマホなどで写真に撮っておくか、メモに書き写して保管しておきます。

次に、セキュリティの設定をします。初期設定時にIDと「ログインパスワード\*1」▶用語集 P.204の設定を必ず行いましょう。また、マニュアルにしたがって起動用「BIOSパスワード」▶用語集 P.190や「ファームウェアパスワード」▶用語集 P.201という、電源を入れた段階で入力することを求められるパスワードも設定しましょう。これを設定しておく、と、盗難されてもOS▶用語集 P.191の起動ができなくなり、盗難時の情報流出をより強固に防ぐことができます。

これらのパスワードは、「ログイ

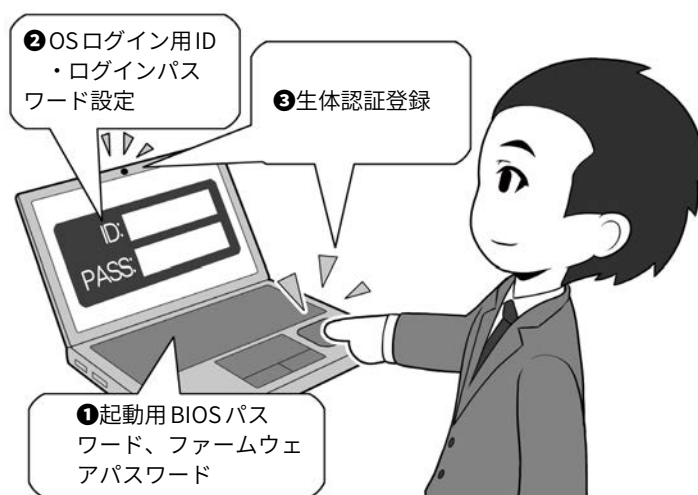
\*1 パスワードにはいろいろな種類があるので、詳しくはP.110以降を参照

### パソコンを買ったらまずリカバリメディアを作る



DVD-RディスクやUSBメモリでリカバリメディアを作り、本体裏などにあるプロダクトキーを撮影し保存します。メディアが添付されていれば作る必要はありません。

### 起動用のパスワードや生体認証登録をしよう



「ログインパスワード」はセオリーどおり複雑なものを設定し、その上で生体認証を使いログインの手間を省くようにします。盗難や不正利用防止のためBIOSパスワードなども設定しましょう。BIOSパスワードなどは「ログインパスワード」相当に設定します。



ンパスワード」のセオリー通り複雑で安全性の高いものを設定してください(P.32,P.110)。生体認証を使用すると、パスワードの桁数が多くて

も毎回入力する必要がなくなるので、ログイン操作が楽になるメリットがあります。

## 2.2 暗号化機能などでセキュリティレベルを高める

パソコンを盗まれたときに、情報が流出しないように、攻撃者からの攻撃が難しくなるようにセキュリティレベルを上げましょう。

会社のパソコンは泥棒などが盗んで帰れないように、ワイヤーロックという盗難防止用のワイヤーで、机などに固定して、持ち運べないようにしましょう。

こういった状態だと、盗みに入った泥棒はパソコンの中の情報だけでも入手すべく、パソコンを壊して中の記憶装置であるハードディスクや SSD ▶用語集 P.192 だけを盗む可能性もあります。

そのように盗まれても情報が漏れないようにするため、記憶装置は暗号化处理 ▶用語集 P.194 を行っておきましょう。

なお、暗号化機能付き外付け記憶装置の場合、使用開始時に入力するのは暗号化の鍵になる「暗号キー」になっているので、「ログインパスワード」より複雑な「暗号キー\*2」のセオリーに従い、英大文字小文字+数字+記号で15桁以上に設定します。

きちんとした複雑さと長さの「暗号キー」で暗号化された記憶装置は、仮に盗んで別のパソコンに繋いでも、解読が非常に困難であり、情報流出を防ぐ力になります。

また、スマホにあるリモート(遠隔)ロックやリモートワイプは、業務用かつ LTE ▶用語集 P.191 などの通信回線を内蔵している一部のパソコンでも可能です。とくにこういった用途を前提に開発をされている機種は、相手から電源が入っているように見えない状態で記憶装置の中身を消すこともでき、重要情報を持ち出す必

\*2 暗号キーに関しては、詳しくは P.110 以降のパスワードに関する項目を参照

### 盗難にそなえて記憶装置の暗号化



TPM チップ ▶用語集 P.193 (≡暗号化チップ) で暗号化されている記憶装置は、「暗号キー」が元の本体の TPM チップ内に残されているので、盗み出しての暗号化解除がさらに困難になります。

### パソコンでもリモートワイプはある



業務用の一部機種では、起動をさとられないステルス状態 ▶用語集 P.197 で、リモートワイプ(遠隔操作でパソコンの中身を消去)などが可能です。盗んだ相手が気づく前に処置することができます。もちろん、そもそも盗まれないようにするのが第一ですが。

要がある場合は有効な防御手段となります。

スマホほどの精度ではありませんが、こういったパソコンでは GPS ▶用語集 P.191 無しでも盗まれた機器の現在

地を探索することもできるので、置き忘れのままや届け出られてる場合は取りに行き、盗まれている場合は情報を添えて警察に相談しましょう。



## 2.3 マルウェア感染に備え、3-2-1のバックアップ体制を整える

マルウェア▶用語集 P.203 の感染に負けない環境を整えるにはシステムやソフトウェアを最新の状態に保つこと、セキュリティソフト▶用語集 P.198 を導入し同様に最新の状態に保つことが重要です。しかし、それでも感染してしまったとき、素早く復旧させるためには、定期的なデータのバックアップが重要です。

バックアップは「3-2-1 ルール」といって、本体含め3個以上の複製、2種類以上の記録メディアで、1個は遠い場所に保管することを推奨します。具体的には、パソコン+バックアップ用記憶装置+クラウドサーバといった形です。

メインのバックアップ用記憶装置は外付けで、最低でも内蔵記憶装置の3~4倍の容量にして、何世代分かのバックアップを可能にすることが理想です。昨今顕著になってきた、パソコンの中のファイルを勝手に暗号化し、解除するには身代金を要求するマルウェア(ランサムウェア▶用語集 P.203)に備えるために「定期的にバックアップをしつつ、普段は本体に接続しておかない」という、やや煩雑な対応が必要です。こうすることでバックアップ用記憶装置もろとも暗号化されてしまうことを防げます。

また、とくに重要なデータは、信頼できるクラウドサーバ上にセキュリティを固めた上でバックアップして、地震、火災、水害などの災害に遭っても重要なデータが巻き添えにならないようにしておきましょう。

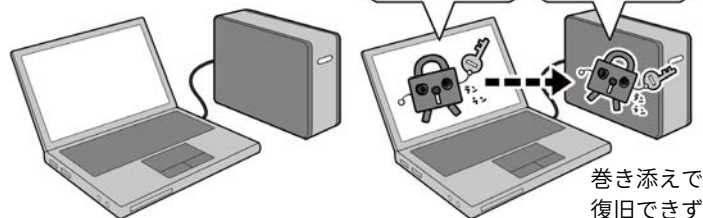
ランサムウェアをはじめ、こういったマルウェアの感染はネット経由だけだと思われがちですが、それだけでは限りません。

### バックアップの体制を整え、普段は接続しない

外付けバックアップ用記憶装置は最低でも内蔵記憶装置の3~4倍の容量のものを手配する

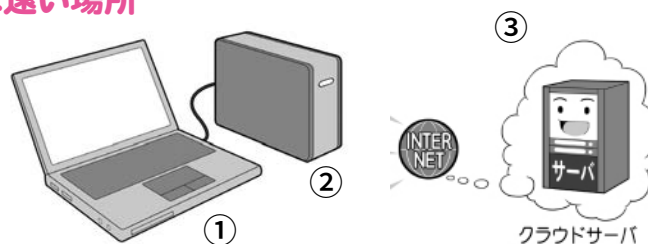
お、バックアップ用記憶装置発見！暗号化しちゃえ

バックアップ用記憶装置暗号化完了



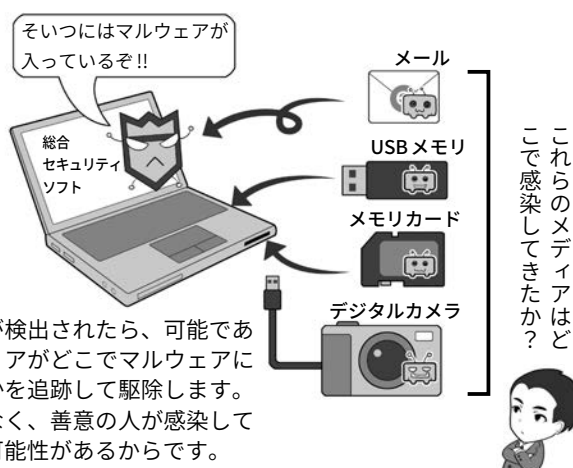
環境を整えたらシステムのバックアップを開始します。ソフトウェアの導入や環境の変更があればバックアップします。システムのアップデート後もバックアップします。ただし、バックアップ用記憶装置を常に接続しておくとランサムウェアに感染して巻き添えて暗号化され、復旧に使うためのデータも失われてしまうので注意が必要です。

### バックアップは3個以上、2種類以上の記録メディア、1個は遠い場所



このルールは、①本体+②バックアップ用記憶装置+③クラウドサーバで条件を満たせます。クラウドサーバは多要素認証、USB セキュリティキーなどを使って攻撃者に乗っ取られないようにしましょう。暗号化が可能なら暗号化して、共有設定をしっかりと確認しましょう。

### さまざまなマルウェア感染源に注意する



マルウェアが検出されたら、可能であればそのメディアがどこでマルウェアに感染してきたかを追跡して駆除します。攻撃者だけでなく、善意の人が感染している可能性があるからです。

例えば、仕事相手の会社の人から「資料をコピーしてくれ」と渡されたUSBメモリにマルウェアが仕込まれていたり、パーティでプレゼント

されたデジタルカメラに仕込まれていたりというケースも実際に存在します。注意しましょう。



## 2.4 売却や廃棄するときはデータを消去する

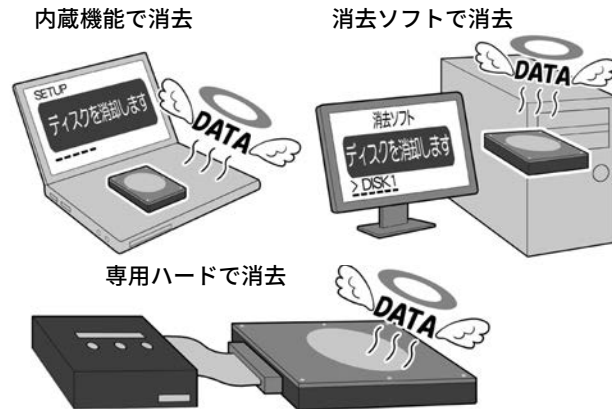
パソコンの廃棄にあたっては、機密情報などの情報漏えいを防ぐために、内蔵記憶装置のデータを復元できない形で消去しなければなりません。とくに個人情報などを扱う場合は、個人情報保護の観点から、廃棄時は確実に情報を消去する努力義務が求められています。

内蔵記憶装置が正常に読み書きできる状態で、パソコン本体にディスク消去機能があるなら、それを使い消去。無い場合は、消去用のソフトウェアを利用。記憶装置単体で保管していた場合などは本体に接続して消去するか、専用の機器などで消去。

データの最低限の消去は記憶装置全域に無意味な情報を書き込むことで、記録されていた情報の残留の可能性を消す方法が考えられます。かつて米国国防総省や軍などでは、3~4回以上の繰り返し上書きによる消去を推奨していましたが、2014年に米国の政府機関 NIST (National Institute of Standards and Technology 米国国立標準技術研究所) が発表した「NIST Special Publication 800-88 Revision 1 Guidelines for Media Sanitization」(<https://csrc.nist.gov/publications/detail/sp/800-88/rev-1/final>) によると、上書き回数は1回でも十分で、専門機関であっても上書きされたハードディスクの復旧は困難、という見解が発表されています。ハードディスクの場合これに従わないと、消えたように見えたデータを復旧できる可能性が残るのです。

なお、SSD はデータの管理方式がハードディスクとは異なるので、生産メーカーの「Secure Erase」用ソフ

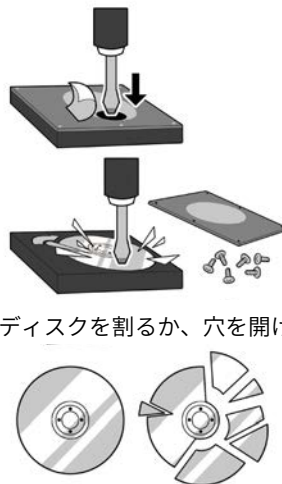
### 記憶装置の中のデータは必ず消去する



ハードディスクは、いずれの場合も最低1回以上の繰り返し消去（データ上書き）処理をするモードを選択します。SSD はメーカー製の消去用ソフトなどを使います。

### 動作不能、機密性確保には破壊する

- ①ハードディスクは破壊用の穴を使うか、分解してディスクを取り出し壊す
- ②目の前で破壊してくれる店に持ち込む(有料)



中のディスクを割るか、穴を開ける



物理的もしくは磁気的に破壊できる機器を購入する（企業など向け）

ガラス製のディスクならば割れば OK です。金属製ならばドリルを利用して穴を開け読み出し不能にします。壊れて動かなくても、記録ディスクだけを他に移植して読み出すという手段があるので確実に破壊しましょう。SSD は中のメモリチップを物理的に破壊するのが理想です。

トを探してこれらを利用するなどの方法があります。

故障して正常に読み出せない、あるいは機密性を求められるもの場合は、物理的もしくは磁気的に破壊する方法もあります。

有料ではありますが、家電量販店などに破壊サービスがあります。こ

れらは自分が見えるところで破壊してくれるので確認しましょう。

企業などで多量に廃棄する場合、安全が確保された環境でハードディスクを読み出し不可能に破壊するか、ハードディスクや SSD でも粉碎できるシュレッダーの導入も検討しましょう。情報漏えい防止の投資です。

## 2.5 紛失・盗難のとき、スマホとパソコン、どっちが安全？

紛失・盗難という視点から見たときに、スマホとノートパソコンとデスクトップパソコン、どれがより安全なのでしょう。

おかれている環境にもよりますが、「盗まれた後」までをその要素に入れて考えてみます。

図のとおり、人目に付きやすいスマホは当たり前ですが盗みやすく、その代わり盗難時の不正なロック解除は困難。また、基本的に通信機能があり、落とした後の位置情報の確認や盗まれたときのリモートロックやリモートワイプ機能といったセキュリティ機能が標準で備わっています。

ノートパソコンはログインパスワードの試行に制限が無い場合もあります。一方、PINコードや指紋認証型もあります。盗難された場合に場所を特定し取り戻すにはLTEなどの「通信機能内蔵型」が現実的な最低条件となり、現状ではほとんどの機種で利用できないので、紛失・盗難した後の探知が困難です。




デスクトップパソコンは基本的に屋内にあるのと、建物の施錠やワイヤーロックによる固定も可能であり、仮に盗難したとしてもノートパソコンと比較して目立たないように持ち出すのは困難です。したがって、盗

難後の探知機能も通常は搭載していません。さらには、入出管理システムや監視カメラの設置、物理ICカードを用いた未使用時のロックなどで盗難への安全性を高められます。

結果として「紛失・盗難時のリカバリ手段や防御手段の少ないノートパソコン」が、紛失・盗難に対し最もリスクといえるかもしれません。

そうなった場合のために、せめて窃盗犯が勝手に起動してデータを読み出すことができないように、BIOSパスワードや記憶装置暗号化の手段を講じておきましょう。

### 要素から安全性のポイントを検証する

	盗まれにくい	人目の目に付きにくい	ロック解除が困難	LTEなどの内蔵通信機能	GPSを使った位置情報	リモートロック リモートワイプ
<b>スマホ(タブレット)</b> 	×	×	○ 生体認証 PINコード 多数失敗で ログイン試行自体を ロック	○	○	○
<b>ノートパソコン</b> 	△	△	△ 失敗しても ロック無しも  ○ 生体認証 PINコード	△ *1  × (回線非搭載)	△ *2  × (回線非搭載)	△ *3  × (回線非搭載)
<b>デスクトップパソコン</b> 	○	○	△ 失敗しても ロック無しも	×	×	×

\*1 LTEなどの無線WAN ▶用語集 P.193 通信機能を内蔵しているものが対象

\*2 LTEなど内蔵機のみ。ノートパソコンの場合はGPSが内蔵されていなくても、通信基地局を使ったおよその位置確認が可能な場合もある

\*3 LTEなど内蔵機のみ。本体が起動していないように見せつつ、リモートロック、リモートワイプを行うことには、専用設計された機種が必要

## コラム.1 ダブルラインでトラブルに備える

インターネットを閲覧していると、突然サーバが無反応になることがあります。そのときどうやって原因を解明するのがよいのでしょうか？

使用しているパソコンやスマホが原因なのか、無線 LAN か、それともウェブサーバ▶用語集 P.194 自身がダウンしているのか。

ネットを仕事に使っているなら、通信ができなくなるのは死活問題。速やかにトラブルを特定し、別経路でのアクセスを確保するテクニックを身につけましょう。

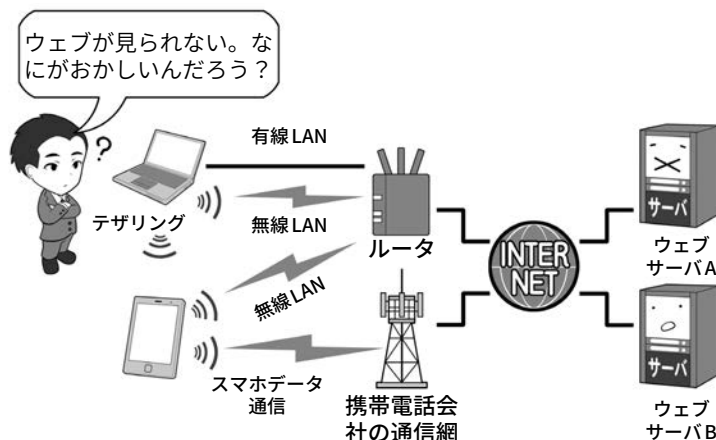
それには主要な機器の二重化(ダブルライン化)が有効です。パソコンで見られないならスマホで確認。無線 LAN がダメならば有線で。ルータ▶用語集 P.204 がおかしいなら LTE で。A というサーバがダメならば B へアクセスして、トラブルが発生した部位の機器を避けるなどの処置をしましょう。

また、所有する特定の機器がマルウェアに感染したり、セキュリティホール▶用語集 P.198 が明らかになったアプリなどを避けてサービスを利用したりする場合も、同様の考え方になります。

特定の機種へのサイバー攻撃が流行っているなら別機種で、ウェブブラウザ▶用語集 P.195 にセキュリティホールがあるなら別のブラウザで。問題があるものを積極的に避けて利用するわけです。

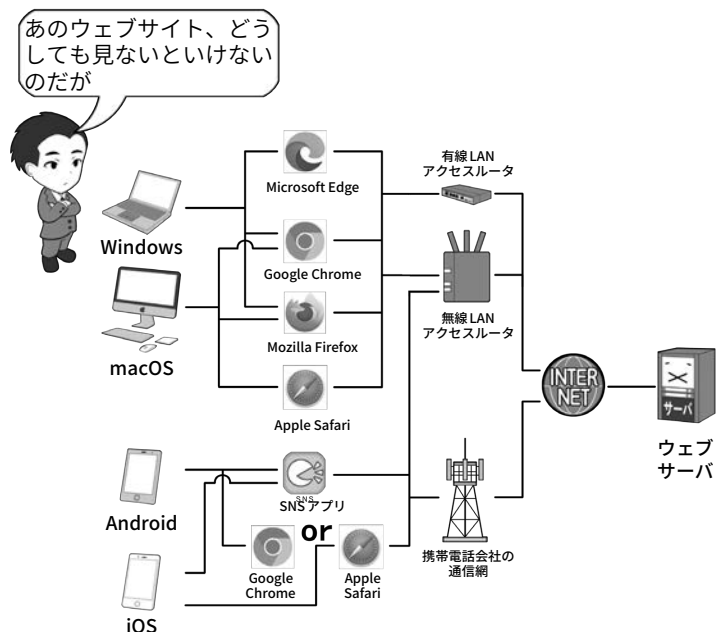
複数台の機材を持つ場合は、機材のタイプを分散することも備えとしては有効でしょう。

### 通信状態がおかしいときに問題点を絞り込む手段



自分から見ると、インターネットのウェブサーバを見る機器、ルータまでの通信方法、インターネットまでの通信方法、そして目的のサーバまで切り替えることで、どの部分にトラブルがあるかを絞り込めます。なお、すべてを切り替えてもネットが表示されない場合は、しばらく時間をおいて確かめましょう。いずれかの場所で通信が集中し混雑して通信ができなくなっている可能性があります。

### パソコンがマルウェアに感染したり、ブラウザがセキュリティホールで使えないときの回避手段



Windows にトラブルが発生したら macOS で、特定のウェブブラウザにトラブルが発生したら別のウェブブラウザで、スマホのアプリにトラブルが発生したらウェブブラウザ版▶用語集 P.202 サービスを利用するなどの回避手段を設けるのも、1 つの防衛策です。

ここでは簡略化して描いているため、上のイラストを含めインターネットの部分で二重化が収束してしまっているように見えますが、そもそもインターネットは通信経路上にあるサーバが攻撃で破壊されても、迂回して通信が確保されるようになっているので、通信が断絶するトラブルがあった場合、自然と迂回路が形成され通信が確保されるはずなのです。

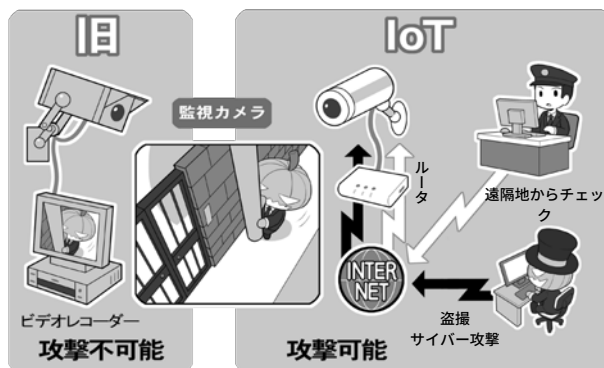
# IoT機器のセキュリティ設定を知らう

## 3.1 常にインターネットに接続するIoT機器は注意が必要

IoT (Internet of Things) ▶用語集 P.191  
 機器とは、従来ネット接続しなかった電気機器が、インターネットに接続可能になったものを指します。例えば、従来の監視カメラはネットに接続する機能を持っていませんでしたが、IoTの監視カメラは撮影した映像をネット経由でスマホなどに送信して危険を通知するなどの機能を備えており、より便利に使うことができます。注意したいのはインターネットにつながるということは、インターネット上にいる、世界中の攻撃者から攻撃対象になりうるということです。例えばIoTの監視カメラであれば、攻撃者がセキュリティホールを突いて乗っ取り盗撮カメラとしても使うことができます。諸外国においては、クラッカー▶用語集 P.195 がIoT機器を乗っ取りボットネット▶用語集 P.203 として悪用し、大規模なサイバー攻撃(DDoS攻撃▶用語集 P.190)を仕掛けたことで、インターネットサービスが停止し、社会経済に深刻な被害が生じた例があります。被害を避けるためには、IoT機器のファームウェア▶用語集 P.201 を最新にしてセキュリティの不備をなくす必要があります。総務省はIoT機器のセキュリティ向上を目指し、「NOTICE」(<https://notice.go.jp/>)というサポートセンターを設置し、ウェブや電話による対応窓口を通じて、IoT機器利用者へ適切なセキュリティ対策を案内しています。IoT機器の

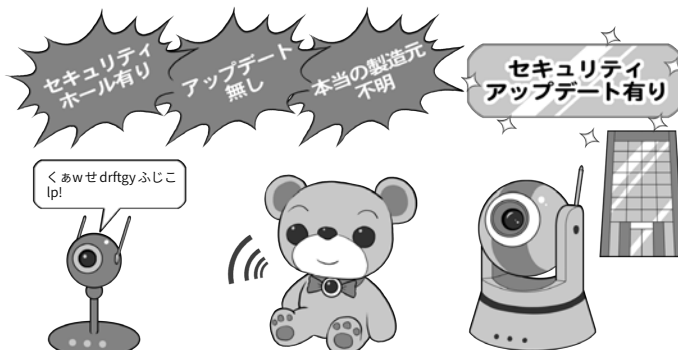
従来の監視カメラはSDカードや有線接続などで内部記憶するタイプが主流で限られた場所でのみしか確認できませんでしたが、IoT機器化することで、遠隔地からチェックできたり、問題が発生すればスマホで通知や映像を受け取ることもできるようになりました。しかし、代わりにサイバー攻撃を受ける可能性も生まれたのです。

### IoT機器に進化するとセキュリティ上のリスクも生む



従来の監視カメラはSDカードや有線接続などで内部記憶するタイプが主流で限られた場所でのみしか確認できませんでしたが、IoT機器化することで、遠隔地からチェックできたり、問題が発生すればスマホで通知や映像を受け取ることもできるようになりました。しかし、代わりにサイバー攻撃を受ける可能性も生まれたのです。

### セキュリティ上、注意が必要な製品も少なくない



悪意ある第三者によって不正な操作が可能なホームカメラ

盗聴・盗撮の脆弱性が指摘された、カメラ付きぬいぐるみ

ネットワーク製品の販売実績が豊富なセキュリティリテラシーの高い企業の製品

IoT機器の中には、セキュリティホールがあっても対処されない、アップデートが提供されるウェブサイトも不明など注意が必要な製品も流通しています。ネットワークに接続する製品は、セキュリティのリテラシーが高い企業製で、なるべく自動更新機能付きのものを購入しましょう。

### NOTICE IoT機器のセキュリティ対策周知啓発

<https://notice.go.jp/>

#### ●NOTICEサポートセンター

0120-769-318 (無料・固定電話のみ)  
 03-4346-3318 (有料)  
 受付時間 10:00～18:00(年末年始12/29～1/3を除く)

#### ●お問い合わせフォーム

<https://notice.go.jp/inquiry>

挙動がおかしいと感じたときは電源を入れ直す、ファームウェアアップデートを怠らずなるべく自動更新の

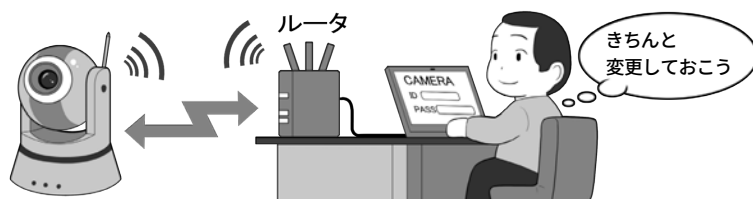
設定しておく、とスマホやパソコンと同様の対策を講じることが重要です。



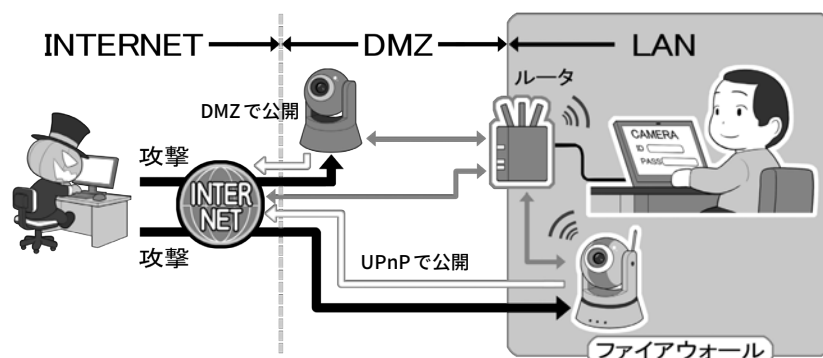
## 3.2 購入後は初期パスワード変更などの設定を

前項のように悪意を持った設計と思われる製品はさておき、その他にも攻撃者の危険にさらされる可能性のある要素は対処しておきましょう。まず、ウェブブラウザで機器の設定画面にアクセスするための、管理者用パスワードは出荷時の状態から必ず変更しましょう。機種によってはそのモデルすべてで同じパスワードが設定されていたりするものもあり、格好の攻撃対象となります。また、ネットワークの設定も適切に行う必要があります。IoT 機器を意図せずインターネットに公開する可能性のある「UPnP」▶用語集 P.193 などの機能は基本的にオフにして、必要な機能を精査して使うようにすべきです。これは社内などのネットワークと外部のインターネットの境目にあるルータでも同様に設定します。IoT 機器は記憶容量が少なく、パソコンなどのように総合セキュリティソフトをインストール▶用語集 P.194 できません。そのためにルータ自体が IoT 機器に対応した、包括的なセキュリティ機能を持つ「IoT 対応セキュリティ機能内蔵ルータ」にしましょう。その中にはパスワードの変更不要な安全な設計のルータもあります。外部からの攻撃だけでなく、IoT 機器が勝手に外部に情報を送信しないように、監視できる体制を整えましょう。ただ、IoT 機器に関する一番のセキュリティ対策は、ネットワークに接続する明確な理由のないときは、そもそも接続しないことです。ワイヤレスイヤホンなどにより普及している Bluetooth 機器についても同様です。使用しないときはオフにして最新版にアップデートしましょう。

### 初期の管理者パスワードは変更する

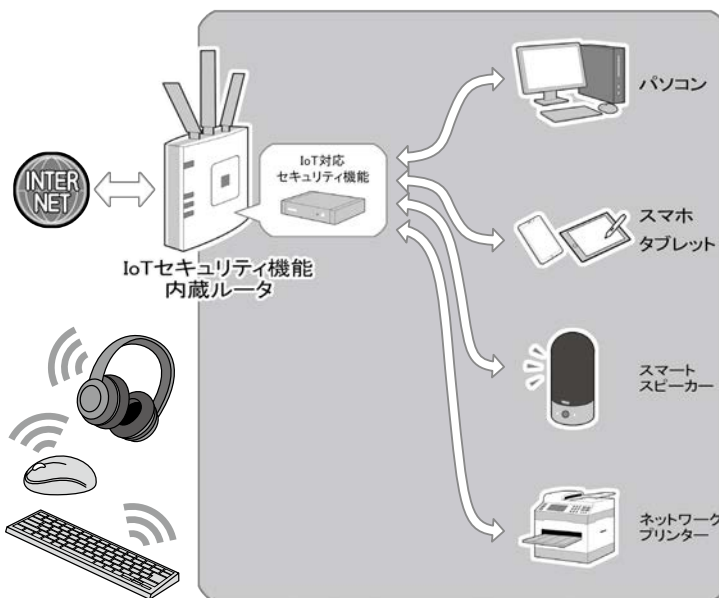


IoT 機器を導入したら不正アクセス防止のため、まず初期の管理者用パスワード（初期パスワード▶用語集 P.197）は変更しましょう。大抵の場合、ウェブブラウザ経由で IoT 機器にアクセスして変更するようになっています。



そのほかにも、インターネットに対して LAN 内部の機器を公開してしまう可能性のある、UPnP 機能はオフにして、インターネット側（DMZ▶用語集 P.190）に IoT 機器を設置することもやめましょう。いずれも攻撃者から IoT 機器へのアクセスが容易になるからです。

### 小さい会社などなら IoT 対応セキュリティ機能内蔵ルータも



IoT 機器、Bluetooth 機器はパソコンやスマホと異なって、記憶容量が小さいためセキュリティソフトなどを導入することがほぼできません。したがってサイバー攻撃に弱く、また、モニターがないため機器の状態をチェックしづらく、乗っ取られてもこれを察知することが難しいのです。そういった状態を察知するために、最近では IoT 機器に対する監視機能を持った装置を、インターネットの玄関口になるルータに接続したり、あるいはルータ自身の中にそういった機能を内包するものがあるので、これらの導入を検討しましょう。こういった装置は IoT 機器など LAN 内の機器を監視し、不自然な点があれば連携したスマホのアプリなどで確認できます。

# それでも攻撃を受けてしまったときの兆候と対処を知ろう

対策を講じサイバー攻撃の大部分を防げても、残念ながら攻撃を受けてしまう可能性をゼロにはできません。攻撃を受けてしまったときの兆候と対処行動を説明しましょう。

まず、システムを最新の状態にしたのち総合セキュリティソフトを入れたとしても安心してはいけません。セキュリティホールの発見に対してアップデートなどの提供が間に合わない状態で、攻撃をしかけられたら、防ぐことが難しいからです。(ゼロデイ攻撃▶用語集 P.198)

備えるだけでなく、攻撃を受けたときの兆候を敏感に察知する能力を身につける意味はここにあります。

攻撃の兆候の中からいくつかの例を挙げてみましょう。

アカウントの乗っ取りの兆候は、知らないログイン通知やログイン履歴、ログインしている機器の一覧に知らないものがあったり、あるいはSNSでの自分が知らない投稿やアプリ連携▶用語集 P.194 などがあります。

銀行口座関連も、ログイン通知があればそれを受け察知したり、通帳や取引履歴を見てチェック。クレジットカードはたとえ少額であっても利用履歴を検証しましょう。

そしてマシンが乗っ取られている場合などは、動作が普段より遅かったり重かったりすることがあります。

もしマルウェアの感染の疑いや、アカウント乗っ取り、情報の流出や不正送金など、実害が判明したら、とりあえずは有線でも無線でもネットにつながる回線から切断した上で、本体の電源はそのままにして、証拠

## セキュリティソフトが検知しなくても、兆候に敏感になれ



## 実被害が出ているときは証拠を保全して通報

### 証拠保全



LANケーブルは抜き、無線LANは本体もアクセスポイントもオフにします。被害拡大防止になります。

### 各所に連絡



### 原因究明までの緊急避難措置



感染したマシンでメールでの連絡や仕事のやりとりは×。感染経路やマルウェアの種類などが判明するまで、同一LAN内、同種の機器の利用も避け、別の種類の機器、別の種類の回線を使います。会社や家のパソコンなどが感染したら、スマホなどの通信回線を使用するなどの暫定的な回避策を行いましょう。

保全を図りましょう。

通信を切断するのはマルウェアの

拡散防止と外部の攻撃者との通信を絶つため、本体の電源を切らない

理由はパソコンなどのメモリ上の証拠を消してしまわないためです。

その後、必要に応じて各種金銭取引関係のサービスを一旦止めてもらう連絡をし、相談窓口などに連絡して対処方法を相談しましょう。また、警察の担当部署に通報・相談しましょう。

侵入経路の解明やマルウェアの駆除が終わるまでは、連絡や仕事のやりとりは、感染が疑われる機器とは別の機器、別の回線を用いて行いましょう。例えば会社や家のパソコンなどが感染したら、スマホなどの通信回線を使用するといった暫定的な回避策です。感染が疑われる機器と同じLANに接続していた別の機器も、感染している可能性は否定できないので使用は控えましょう。

マルウェアが発見されただけで実害が出ていない場合、セキュリティソフトなどで駆除できるときは駆除します。駆除できないときは機器を初期化してバックアップから復元し、再びネットに接続して使用し始める前に、感染や乗っ取りの原因と思われるものをクリアにしましょう。

システムやセキュリティソフトは再度最新の状態か確認し、不審なメールや添付ファイルなどが原因だったならばメールを削除、セキュリティホールになりかねないサポート期間切れの機器やソフト、アプリはアンインストール▶用語集 P.194 し、アプリやサービス連携▶用語集 P.196 の棚卸をして、知らないものや不要なものを解除しましょう。

なお、ウェブサービスのアカウントが乗っ取られてパスワードが変更されてしまった場合は、自分で再設定することはできないので、サービス側に連絡してアカウントを取り戻す処理をしてもらいましょう。

## 実被害が出ていない場合

### マルウェアの駆除

セキュリティソフトなどを最新にしてフルスキャンをかけて駆除します。



### バックアップから復元

セキュリティソフトで対処できない場合は、本体を初期化してバックアップから復元します。



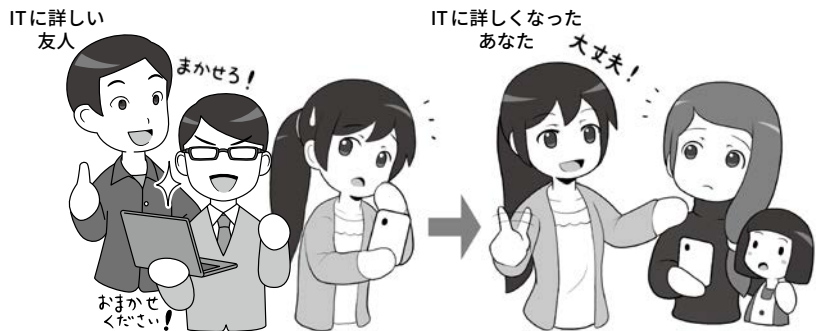
### システムをチェックする



### サービスやアプリ連携の見直し



## 信頼できる相談窓口やITに詳しい友人を頼ろう



困ったときには、信頼できる相談窓口やITに詳しい知人に意見をもらうとともに、自らも勉強しましょう。

そして将来同様のケースがおきたら、あなたが困っている人に「ITに詳しい友だち」として手を差し伸べて、力になってあげてください。

ところで、攻撃が明白でない状況で疑心暗鬼になりそうとき、頼りになるのが、気軽に話せるITに詳しい知人だったりします。相談することで現在おかれている状況が明白になってきたら、各種の相談窓口の連絡や、関係機関への届け出を行いましょう(参照P.175,P.176)。

そのときあなたが誰かに助けられたら、次は誰かを助ける番になって

ください。

1人また1人と、こういったセキュリティに詳しい人が増え、みんなでサイバー攻撃に立ち向かう姿勢が広まることは、きっとネットの安全を守る力になります。



## コラム.2 軍事スパイ、産業スパイに狙われてしまったら

スパイ▶用語集 P.197 ではない攻撃者は、コストパフォーマンスでターゲットを選ぶ傾向がありますが、では逆に職業的なスパイはどのように行動するのでしょうか。

軍事スパイや産業スパイの場合、入手すべき情報は絶対であり、侵入しにくいからといって別の情報にすることや諦めることはできません。

また、こういった攻撃者の場合、活動するための資金を自分でまかなわなくても、国家や軍、スポンサー企業などから活動資金を得ているとコストパフォーマンス度外視で攻撃をしかけられるわけです。

なお、ネットが普及する前のスパイ活動は、相手国の新聞や雑誌など公開されている情報から情報収集するオシント、人間関係を調べたり尾行したり、交友関係を持って情報を聞き出すヒューミント▶用語集 P.201、そして通信を傍受や盗聴して情報を入手するシグントなどがありません。

ネット社会の現代では、SNSを見ればある程度オシントでヒューミント的な情報は入手できますし交友関係も丸わかりです。シグントもターゲットのスマホをマルウェアに感染させれば、メールを盗み見たりファイルを奪取したり、スマホの通話を盗聴できたり、旅行先の状況を盗撮できたりもします。

少なくとも相手がSNS好きの人間なら一般人でも楽にヒューミントもオシントもでき、これがサイバー時代の低コストインテリジェンス(諜報活動)といったところ

### 軍事スパイ、産業スパイに狙われてしまったら

#### 職業スパイにはコストによる防御が効かない

セキュリティの厳重なサーバのイメージ



#### スパイ活動の今昔

昔はスパイといえば…  
オシント (Open Source Intelligence)



地味に販売されている新聞雑誌の切り抜き。ほぼこれ

ヒューミント  
(Human Intelligence)



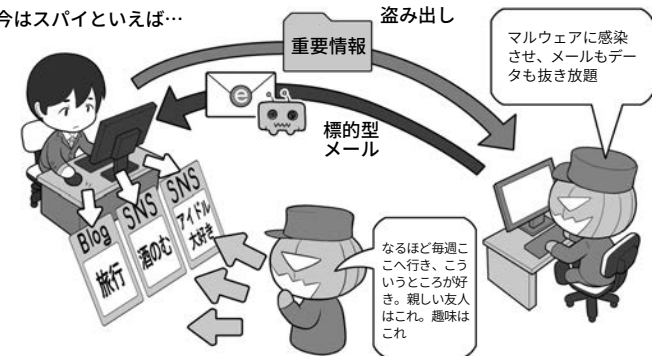
ターゲット  
ヒューミントのための下調べ。尾行して趣味や交友関係を探る

シグント  
(Signal Intelligence)



通信傍受、暗号解読

今はスパイといえば…



デジタルなオシント、ヒューミント

デジタルなシグント

るのでしょうか。

要職にある方々は、SNSなどに不必要に情報を流さないようにしましょう。とくに国際情勢が不安定になると、攻撃は増加する傾向がありますが、基本的な対策はわかりません。

また、2022年には軍事行動を起こした特定国やそのような動き

に呼応した国／有志が、サイバー攻撃をしかける要員をSNSなどで募集するケースも見られました。一般人がこのような募集に応じた場合、攻撃行為が法に抵触する可能性が高い上に、あらぬトラブルに巻き込まれる懸念も出てくることから、応じないほうが賢明といえます。



## 第6章

# パスワードの大切さを知り、通信の安全性を支える暗号化について学ぼう

インターネットを安全に利用するには適切なパスワード管理が不可欠です。また通信の安全性を保つには暗号化技術が役立っています。パスワード管理、知っておきたい暗号化の必要性やしくみを学びましょう。

### 1 パスワードを守ろう、パスワードで守ろう

- 1.1 パスワードってなに？
- 1.2 3種類の「パスワード」を理解する
- 1.3 「PINコード」と「ログインパスワード」に求められる複雑さの違い
- 1.4 「暗号キー」に求められる複雑さ
- 1.5 総当たり攻撃以外のパスワードを破る攻撃や生体認証を使った防御
- 1.6 多要素認証を活用する。ただしSMS認証は避ける
- 1.7 二段階認証と二要素認証と多要素認証の安全性
- 1.8 パスワードの定期変更は基本は必要なし。ただし流出時は速やかに変更する
- 1.9 パスワード流出時の便乗攻撃に注意
- 1.10 適切なパスワードの保管
- 1.11 パスワード情報をクラウドで保管する善し悪し
- 1.12 ノートやスマホを失くした場合のリカバリ考察
- 1.13 注意すべきソーシャルログイン
- 1.14 権限を与えるサービス連携にも注意

**コラム1** 暗号化の超簡単説明

**コラム2** パスワードの管理と流出チェックについて

**コラム3** パスワードを記録する演習

### 2 安全な無線LANの利用を支える暗号化について学ぼう

- 2.1 それぞれの状況に合わせた暗号化の必要性
- 2.2 無線LAN通信 (Wi-Fi) の構成要素
- 2.3 暗号化無しや、方式が安全ではないものは危険
- 2.4 暗号化方式が安全でも「暗号キー」が漏れれば危険
- 2.5 会社などでの安全な無線LANの設定(暗号化方式)
- 2.6 会社などでの安全な無線LANの設定(その他)
- 2.7 公衆無線LAN利用時の注意
- 2.8 個別の「暗号キー」を用いる方式の公衆無線LAN
- 2.9 公衆無線LANに関して新規に購入したスマホなどで行うこと
- 2.10 公衆無線LANが安全ではない場合の利用方法

2.11 自前の暗号化による盗聴対策

2.12 まとめて暗号化するVPN

### 3 安全なウェブサイトの利用を支える暗号化について学ぼう

- 3.1 無線LANの暗号化とVPNの守備範囲
- 3.2 すべての通信と、その一部であるウェブサイトとの通信
- 3.3 httpsで始まる暗号化通信にはどんなものがあるか
- 3.4 より厳格な審査の「EV-SSL証明書」
- 3.5 アドレスバー警告表示と、常時SSL化の流れ
- 3.6 有効期限が切れた証明書は拒否する
- 3.7 他にも証明書に関する警告が出るウェブサイトは接続しない
- 3.8 ウェブサービスのログインは多要素認証を選択する
- 3.9 多要素認証すら破る「中間者攻撃」
- 3.10 ウェブサイトを使ったサイバー攻撃に対応する

### 4 安全なメールの利用を支える暗号化について学ぼう

- 4.1 メールにおける暗号化
- 4.2 送信の暗号化と受信の暗号化
- 4.3 メールにおける暗号化の守備範囲
- 4.4 メール本文の暗号化
- 4.5 怪しいメールとはなにか
- 4.6 マルウェア入りの添付ファイルに気を付ける
- 4.7 ウェブサービスなどからのメールアドレスの流出
- 4.8 流出・スパム対策としての、変更可能メールアドレスの利用
- 4.9 通信の安全と永続性を考えたSNSやメールの利用

### 5 安全なデータファイルの利用を支える暗号化について学ぼう

**コラム4** 「無料」ということの対価はなにか

**コラム5** クラウドストレージサービスからの情報流出。原因は？

## 1

パスワードを守ろう、  
パスワードで守ろう

## 1.1 パスワードってなに？

私たちが、スマホやパソコンなどのIT機器や、各種のウェブサービスを使う上で、欠かせないのが「パスワード」です。

機器やウェブサービスを利用するときに、正当な利用者や持ち主である自分だけが利用でき、他人が利用できないようにするための鍵の役割を果たすものです。

パスワード▶用語集 P.200 は、いわば「家の鍵」や「金庫の鍵」。これを適切に守らなければ、家や車、金庫を勝手に開けられてしまうように、パソコンやスマホ、ウェブサービス上にある私たちの個人情報やメール、銀行口座が攻撃者▶用語集 P.196 に不正にアクセスされ、情報が流出したり、お金を盗まれたりしてしまいます。

なお、こういった役割を担うものには、他に「暗証番号」などや、通信している情報やパソコン・スマホの中のデータを暗号化▶用語集 P.194 して、他人や攻撃者が読めないようにする、「暗号化と復号▶用語集 P.202 の鍵＝暗号キー▶用語集 P.194」というものもあります。

この3つは、性格や役割が異なるのですが、よくまとめて「パスワード」と記述されることがあるのと、暗証番号、パスワードと暗号キーは、等しく攻撃の対象になるために、ここでは一括して扱います。

## 1.2 3種類の「パスワード」を理解する

私たちは、機器やウェブサービスを利用するとき、あるいはファイルを開くときに入力するものを、まとめて「パスワード」と呼び、同じような役割をするものと思いがちです。しかし、セキュリティ上の性質から、「パスワード」とまとめて呼ばれるものは、大きく3つに分けて理解する必要があります。

1. 銀行のキャッシュカードやクレジットカードの利用時や、スマホのロック▶用語集 P.204 解除時に使用し、通常4桁から6桁以上の数字だけで構成されることが多いもの(暗証番号やPIN、PINコード▶用語集 P.191、パスコード▶用語集 P.200。通信事業者のネットワーク暗証番号▶用語集 P.200 などを含む)
2. パソコンやデジタル機器、ウェブサービスなどの利用時にID▶用語集 P.191 とセットで入力し、英大文字小文字、数字、記号を用い複雑さと一定以上の長さが推奨されるもの(狭い意味でのパスワード、ログインパスワード▶用語集 P.204)
3. パスワードと呼ばれていることもあるけれど、本当はファイルや通信内容を暗号化した復号するための暗号鍵▶用語集 P.194 として単独で用いられるもの(ZIPファイル▶用語集 P.193 のパスワード、WordやExcel、PowerPointの保護パスワード、Wi-Fi▶用語

集 P.193 機器の暗号化キー▶用語集 P.194、暗号キー、パスフレーズ▶用語集 P.200、セキュリティキー▶用語集 P.198、ネットワークキー▶用語集 P.200)

一口にパスワードといっても、上記のとおり、実にさまざまなものがあります。P.32でご紹介したのは、上記のうちの2にあたります。

この本では、以降、この3つを混同しないように、

**1を「PINコード」**

**2を「ログインパスワード」**

**3を「暗号キー」**

と呼びます。

## 1.3 「PINコード」と「ログインパスワード」に求められる複雑さの違い

P.32では、機器やウェブサービスを利用するとき、「ログインパスワード」として、英大文字小文字＋数字＋記号混じりで少なくとも10桁以上を推奨しました。

一方、同様に使う「PINコード」は、メーカーが数字のみの4桁から6桁以上でよいとしています。

この2つは、両方とも機器やウェブサービスを利用するときに使用するのに、求められる長さや複雑さに差があるのはなぜでしょうか。

そもそもパスワードに「複雑さ」が求められる理由は、攻撃者が制限のない状態でパスワードの文字列を総当たりで試すと、時間はかかるが「いつか必ず探り当てることが可能」だからです。これは、どんな複雑な「ログインパスワード」でも変わりませ

ん。

こうやって力業でパスワードを探り当てる攻撃を「総当たり攻撃(ブルートフォース攻撃)」▶用語集 P.198 と呼び、「ログインパスワード」を守る第一歩は、いかにこれを成功させないかにあります。

スマホの「PIN コード」の場合は、数回間違えると「入力遅延」といって一定時間「PIN コード」を入力できないようになり、さらに「10回間違えば以降PIN コード入力不可にする(ロック)」(場合によっては機器を初期化する(ワイプ▶用語集 P.204))ことで「総当たり攻撃」を不可能にし、攻撃者による不正利用を防ぎます。

さらに、厳しいキャッシュカードなどでは、3回間違えると以降カードが利用できなくなりますが、これも同じ考え方です。

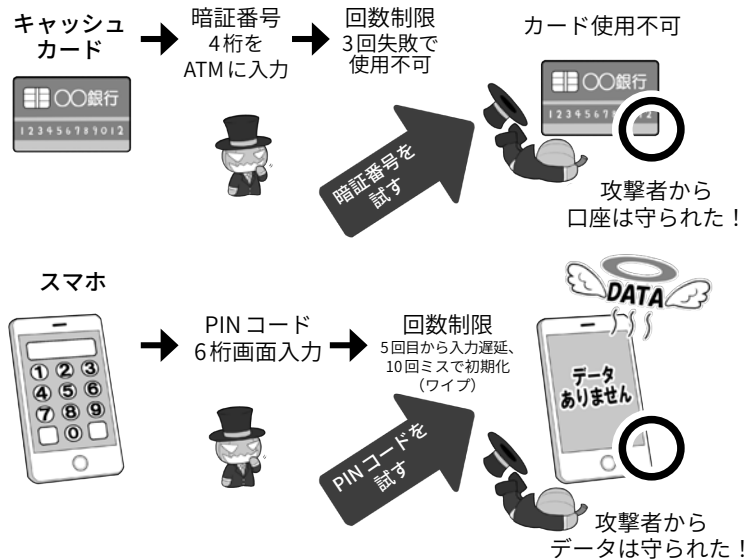
「PIN コード」では、こういった厳しい制限を設けることで「総当たり攻撃」を不可能にし、4桁から6桁以上の数字でも攻撃者から機器やサービスを守れるのです。

一方、「ログインパスワード」は、通常「PIN コード」のようにワイプまでする機能がついていることは、ほぼありません。数回失敗すると入力間隔が開く、一定時間入力をロックするなどのペナルティを受ける場合もありますが、ペナルティがないものも多いのです。

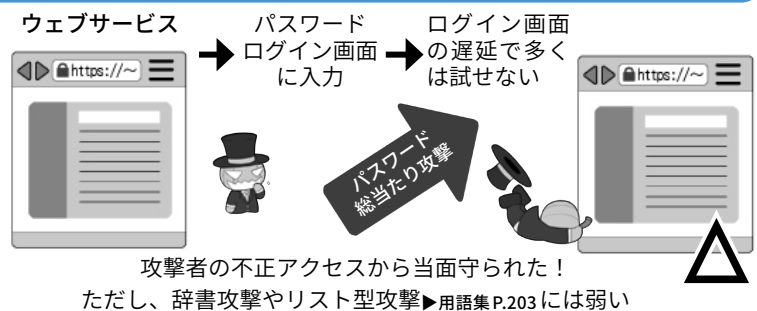
この「ログインパスワード」は、ウェブサービスのログインページや、パソコンやIoT 機器▶用語集 P.191 のログイン画面に入力するもので、こういった入力画面では、ネット経由でログイン▶用語集 P.204 を試みた場合、どう頑張っても1秒に数回~数十回程度しか入力することができず、これだけで実質的に高速な攻撃を防ぎます。

### 3種のパスワードを理解する

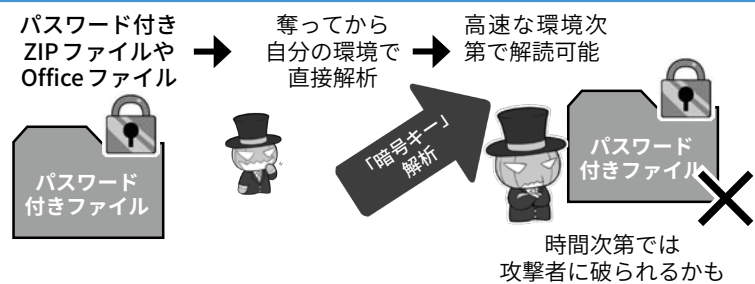
#### ①「PIN コード」の基準で安全性を保てる例



#### ②「ログインパスワード」の基準で安全性を保てる例



#### ③「暗号キー」の基準で安全性を保てる例



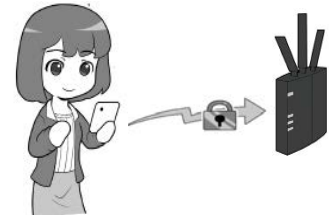
#### 一見、安全性を保つための基準がわかりにくい例

内蔵記憶装置暗号化の救済が必要になる場面



「ログインパスワード」基準の複雑さで安全性を保てそうに思えるが、実際には入力遅延による防御が働かないので「暗号キー」の基準を採用すべき(P.112 で理由解説)。

無線 LAN▶用語集 P.203 アクセス時に入力するパスワードを決める場面



ルータ▶用語集 P.204 にログインする際のパスワードは「ログインパスワード」でよさそうだが、「暗号キー」の基準で設定した方がよい(P.112 で理由解説)。

※この図は一例であり、実際の機器の条件とは異なります。

本書の推奨どおり、英大文字小文字＋数字＋記号 26 種＝88 種類の文字を使い、10 桁のパスワードを作ったとすると、その組み合わせは約 2785 京個(京は兆の上の単位)、1 秒 5 回の制限で「総当たり攻撃」をした場合、全部を試すまでに約 1760 億年かかるわけです。

これならば、100 年以内に探り当てられる確率は非常に小さく、事実上不可能といえるわけです。

このような攻撃の想定を、セキュリティ用語的には「オンラインアタック(攻撃)」▶用語集 P.195 といいます。ここでは「『ログインパスワード』への攻撃」と呼ぶことにします。

#### 1.4 「暗号キー」に求められる複雑さ

上記の「ログイン画面」に入力する「ログインパスワード」とは異なり、「暗号キー」の場合は、攻撃者が暗号化されたデータを盗んで持ち帰り、ログイン画面の遅延などなく、自分のペースで高速な暗号化解除(解読)の攻撃ができます。

この攻撃の対象となるのは、「1 つ、または複数のファイルを圧縮したパスワード付き ZIP ファイル」、「パスワードを設定した Microsoft Office のファイル」、「暗号化された USB メモリ」や「パソコンから取り出された内蔵補助記憶装置▶用語集 P.203(ハードディスクや SSD▶用語集 P.192。以下記憶装置▶用語集 P.195)」,あるいは「暗号化された無線 LAN 通信の内容」などです。

こういったものでは、「パスワード」と思って設定しているものが、実はパスワードではなく、中身を読まれないようにするための暗号化に使われる鍵＝「暗号キー」となってい

る場合が多いのです。

ZIP や Microsoft Office のファイルは、パスワードが設定されていると、開くときにパスワード入力画面が出るので、入力遅延の防御があるように見えますが、実はその画面は ZIP や Office のプログラムが提供しているもので、ファイルそのものは単なる暗号化されたデータにすぎないのです。

そのため、パスワード入力画面を使わなくても直接ファイルに対して暗号化解除の攻撃が可能であり、遅延による防御はありません。

このような暗号化解除は、「暗号キー」が短いと、スーパーコンピュータを使うまでもなく、市販されているゲーム用パソコンの性能で十分可能なレベルの難易度なのです。少し古いデータになりますが、2019 年ごろの一般流通するゲーム用パソコンでもグラフィックボードに搭載されている GPU というプロセッサを駆使すれば、ZIP ファイルに対して 40 億回/秒の暗号化解除の攻撃が可能というデータすらあります。さきほどの約 2785 京個の組み合わせがある場合でも、解読までにかかる期間は 78.5 万年に短縮、8 桁のものになると 103 年、8 桁で記号抜きの 62 種の文字だと 6 年、英大文字小文字だけだと 2 年となります。短く単純なパスワードなら短時間で解読可能でできてしまう、GPU の性能が向上すればそのような日がいずれ訪れても不思議ではありません。そのため本書では、「暗号キー」には、完全にランダムで英大文字小文字＋数字＋記号混じりで 15 桁以上のものを推奨し、これを基準とします。

ZIP のパスワードに、15 桁ものランダムな文字列を使うのは、覚えられなくて無理だと思われるでしょう

が、8 桁程度のパスワードでは破られてしまうので、暗号化したつもりでも攻撃者の前では意味がないのです。なお、このような想定 of 攻撃をセキュリティ用語的には「オフラインアタック(攻撃)」▶用語集 P.195 と呼びますが、ここでは「『暗号キー』への攻撃」と呼ぶことにします。

#### 1.5 総当たり攻撃以外のパスワードを破る攻撃や生体認証を使った防御

パスワードなどを破る攻撃には、「総当たり攻撃」の他にもさまざまな手法があります。

パスワードでよく使われる言葉などを集めた、専用の辞書を利用する「辞書攻撃▶用語集 P.197(ディクショナリアタック▶用語集 P.199)」,ウェブサービスなどから流出した名簿や ID とパスワードのリストを入力して試す「リスト型攻撃(アカウントリスト攻撃・パスワードリスト攻撃▶用語集 P.201)」など。

これらに対する防御のためにも、「ログインパスワード」には意味のある単語や、自分に関連の深い語句やよく使われるパスワードは避け、推奨する基準に従い、十分に複雑で、かつ他の機器やウェブサービスで使い回していないものを設定しましょう。

「PIN コード」は、入力を間違え続けると「入力遅延」や「ロック」機能があるため、「総当たり攻撃」などの手法が有効ではありません。

しかし、「PIN コード」の強さは「盗み見や、推測されないこと」が前提ですので、入力するときは周りに気を配り、また、自分の個人情報など推測しやすいものは使わないようにしましょう。

現に、ATM でお金を下ろすときに、



「暗証番号(PINコード)」を肩越しに覗き盗み取る手口は、「ショルダーハッキング」としてよく知られています。

「PINコード」の盗み見などを防ぐためには、指紋認証や顔認証などの「生体認証」▶用語集 P.198 を利用するのも1つの手です。それらなら肩越しに見られても、攻撃者が容易にまねをすることはできないからです。

ただ、指紋認証などの生体認証も100%安全とは言い切れません。最近では、どこかで撮影した相手の指の写真から、3Dプリンターで偽の指紋を作って認証を突破したり、顔を印刷した紙を加工して、それを使って顔認証を突破したりする実験も行われています。

また、指紋認証が携帯電話に登場したときから、本人が寝ている間に、勝手に指を押し当てて認証を突破するという話があります。最近では、親が寝ている間にこどもが勝手に認証し、ゲームに課金していたという例もありました。したがって、指紋認証だから、絶対安心と過信しないことが重要です。

生体認証はこの他にも、目の虹彩▶用語集 P.196 の模様によって認証する「虹彩認証」、手や指の静脈のパターンで認識する「静脈認証」などがあり日々進化しています。それぞれの特徴やセキュリティ上のメリットをよく検討して利用しましょう。

「暗号キー」は、攻撃に遅延がないので、「総当たり攻撃」を含めすべての攻撃が有効です。また、攻撃されるまでもなく、そもそも「暗号キー」が漏れていれば暗号化された中身が解読され、ひとたまりもありません。この暗号キーが、事実上漏れた状態になる話は、P.124以降で詳しく説明します。

## パスワードを破る手段は色々

### 総当たり攻撃 (ブルートフォース攻撃)



すべての文字列の組み合わせを試す

### 辞書攻撃 (ディクショナリアタック)



パスワードでよく使われる単語を使って試す

### リスト型攻撃(アカウントリスト/ パスワードリスト攻撃)



名前やIDとパスワードの流出リストを使う

あくまでも代表的なものの例ですが、簡単なパスワードやよく使われるパスワードだったり、使い回しをしていたり、流出したのに放置していると、攻撃者に楽々突破されます。パスワードはしっかり管理しましょう。

(本当は、図のように人力ではなくプログラムなどで自動的に行われます)

## 指紋認証が破られることも…



極端な例ではありますが、高度なハッキングをしなくても、酔っ払って寝ているあなたの指に押し当てただけで指紋認証は突破できてしまいます。

指紋認証だから、絶対安心と過信しないようにしましょう。

場合によっては、機器を再起動したり、わざと数回指紋認証を失敗して、強制的に生体認証ができない状態にする対策も検討しましょう。

### 1.6 多要素認証を活用する。 ただしSMS認証は避ける

IDとパスワードでの認証に、さらにチェック機能を追加するのが二要素認証や多要素認証▶用語集 P.198 と呼ばれる機能です。これを利用することで、パスワード流出時の乗っ取りをより困難にします。

最も一般的な方法は、なんらかの手段で入手する、その場限りの「ワンタイムパスワード」▶用語集 P.204 の入力を追加する方法です。ログインに当たって、サービス提供者から、SMS(ショートメッセージ)▶用語集 P.192 や電子メールで送られてくるものを利用する方法や、スマホのアプリ

▶用語集 P.194 を使って生成するソフトウェアトークン▶用語集 P.198 や専用の小さな乱数を発生するハードウェアトークン▶用語集 P.200 を利用する方法、そして物理的なUSBセキュリティキー▶用語集 P.193 や生体認証を用いる方法があります。このうち、SMS方式は海外で乗っ取りからの成りすまして破られた例があり、電子メールも経路上で奪取される可能性があるため、自分で種類を選択できる場合は、トークン、USBセキュリティキー、または生体認証方式を推奨します。

ソフトウェアトークンは、専用のアプリを利用するものと、QRコードを使って情報を読み込むものがあ

り、後者はパスワード管理アプリで一括して管理できる場合もあるので、活用しましょう。

スマートウォッチ▶用語集 P.197 によっては、スマホのパスワード管理アプリと連携して、手でIDとパスワードを確認したり、ワンタイムパスワードを発生させたりできる機種もあります。

また、パスワードをネット経由で送信せず、USBセキュリティキーや生体認証を用いて端末内で本人確認をし、認証したという情報だけを送信する FIDO▶用語集 P.190 などの方式の採用も推進されています。より安全

な利用のために、アンテナ高く認証にまつわるセキュリティ情報を収集しましょう。

## 1.7 二段階認証と二要素認証と多要素認証の安全性

この認証のために用いる要素には下図にあるように、「知っていること」「持っているもの」「本人自身の一部」などの種類があり、このうち最初の認証に用いなかった要素と組み合わせ、二要素以上を用いた認証方式を構成することが重要です。

複数の要素を使用するものを多要素

素認証、その中でもとくに2つの要素を使用するものを二要素認証と呼びます。本冊子では、その意味で推奨する認証方式を「二要素以上の多要素認証」という表現をします。

一方、アカウント認証に関する記事などでよく用いられる言葉に「二段階認証」▶用語集 P.200 というものがあります。これは、認証のプロセスを二段階に分けて行うものであり、構成する要素とは関係がありません。

したがって、二段階認証であっても一要素認証もあれば、一段階認証であっても二要素認証の場合もあり、前者よりは後者の方が安全性が高まります。

また要素のうち、「持っているもの」「本人自身の一部」は、物理的な存在であるため、例えば攻撃者がこれを突破しようとする、物理世界で窃盗や脅迫を行わなければならない、ネットの影に隠れたまま行える犯罪よりもリスクが高くなり、安全性が高まります。

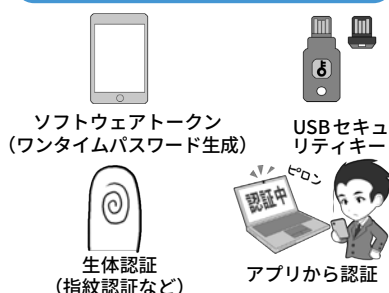
それでも、「知っていること」と「持っているもの」の組み合わせであるキャッシュカードが、オレオレ詐欺などであっさり奪われたり、P.165に解説しますが、多要素認証すら破る「中間者攻撃」も存在したりするため、多要素認証だからそれだけ絶対安全と思ひ込まないでください。常に「自分は、狙われているかもしれない」「攻撃されているかもしれない」「もしかしたら、これは攻撃かもしれない」という危機意識を持つようにしてください。

## 1.8 パスワードの定期変更は基本は必要なし。ただし流出時は速やかに変更する

利用するサービスによっては、パスワードを定期的に変更することを

### 現時点で推奨できる多要素認証要素

#### 基本的に推奨できるもの



SMSを使ったワンタイムパスワード受信は、海外でSIMハイジャック▶用語集 P.192 という攻撃により破られた例があります。また、メールも同様にパスワードを「送信する」という点で攻撃の余地が多くなります。

#### 推奨できないもの



### 多要素認証の構成要素は？

#### ①知っているもの ②持っているもの ③本人自身に関するもの



#### 多要素認証の組み合わせ例



多要素認証は上記の2つ以上の要素を組み合わせます

一方、二段階認証は、二回認証を行います。その要素は多要素とは限らないため、防御力としては弱くなります。

なお、多要素認証のうち、2つの要素だけ用いて認証するものを、「二要素認証」といいます。

求められることがあります。しかし、前出のように十分に複雑で使い回しのないパスワードを設定した上で、実際にパスワードを破られアカウントを乗っ取られたり、サービス側から流出したりした事実がないのなら、基本的にパスワードを変更する必要はありません。

むしろ、パスワードの基準を定めず、定期的な変更のみを要求することで、パスワードが単純化したり、ワンパターン化したり、サービス間で使い回しするようになることが問題となります。

一方、アカウントが乗っ取られたり、流出の事実を知った場合は速やかにパスワードを変更し、その原因も特定しましょう。

原因が、マルウェア▶用語集 P.203などでパソコン側から情報が流出し続けている場合、その穴を解明しないまま放置していると、パスワードを変更しても意味がありません。

また、アカウントが完全に乗っ取られてしまったら、ウェブサービスに連絡して復旧しましょう。

一方、自分の使用機器からではなく、ウェブサービスなどの側からパスワード流出が起きた場合は、速やかにパスワードを変更の上、流出の原因となった点の対策が行われたかを確認しましょう。

サービス側からパスワード強制リセットの通知や、再設定のリクエストが来たら、次項の便乗攻撃に注意しつつ、同様に速やかにパスワードを変更しましょう。

## 1.9 パスワード流出時の便乗攻撃に注意

サービス側から、パスワード再設定の通知がメールなどで送られて来

た場合、まずそれが本当にサービス側から送られてきたものかどうか、該当のサービスのウェブサイト▶用語集 P.194やニュースサイトでチェックし、事実の確認をしましょう。

サービス側を装ったパスワードリセットの通知は、流出事故に便乗したフィッシング詐欺などのよくある攻撃パターンです。パスワードを奪う攻撃者の罠かもしれません。通知のメールにパスワードリセットのリンク▶用語集 P.204などが貼られていても、うかつにクリックしたりせず、リセットする場合も直接公式サイトやアプリからしましょう。

なお、ウェブサービスを利用するときは、パスワードが流出した場合に簡単にアカウントを乗っ取られな

いように、必ず二要素以上の多要素認証を設定しておきましょう。これが提供されないサービスは、セキュリティ意識が低い可能性があるのでそのサービスの利用は再考しましょう。

## 1.10 適切なパスワードの保管

さて、日常的にインターネットを利用していると、IDとパスワードは無限に増えていきます。どう管理すればよいのでしょうか。

本書では、「スマホ用のパスワード管理アプリ」か「物理的な紙のノート」の利用を推奨します。

スマホのパスワード管理アプリを導入する場合は、ネットにデータを

### ウェブブラウザにはパスワードを保存しない

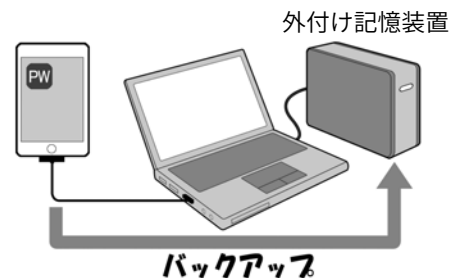


ウェブブラウザ▶用語集 P.195にパスワードを保存すると、席を離れた際に勝手に利用されたり、パソコンをクラッキング▶用語集 P.196された際に根こそぎ盗まれる可能性があります。

### パスワード管理方法の例

一見分かりにくい  
紙のノートに二重で

管理アプリのデータは、暗号化した記憶装置にバックアップ▶用語集 P.201



紙のノート二冊に記入したり、スマホのパスワード管理アプリを使って、パソコン経由で暗号化した記憶装置にバックアップする方法があります。紙のノートは一見内容が分からないようにできる専用のパスワードノートも売られています。



置く「クラウド連携(バックアップ機能)」を安易に利用せず、まずはスマホ内だけで管理する「スタンドアロン」▶用語集 P.197 状態で利用できるものを優先しましょう。

紙と比較した場合、スマホはネットに接続されているので、攻撃者にクラッキングされる可能性は捨てきれませんが、利用規約を守り、システムを最新に保っている限りは、スマホのセキュリティは十分に高い設計となっています。

また、紛失や盗難に遭っても、最新のスマホはデータを暗号化した状態で保存していますし、パスワード管理アプリも独自に暗号化するので二重に暗号化された金庫での保管に等しくなります。加えてスマホは、事前にきちんと設定しておけば、紛失や盗難に遭っても遠隔操作でロッ

クして操作できなくなったり、場合によってはワイプ(消去)して情報流出を避けたりできるという、紛失に対する三重四重のセキュリティが設けられています。

一方、紙のノートを推奨する理由は、あたりまえではありますが、紙のノートはネットに接続できないからです。接続できなければネット経由のサイバー攻撃も不可能です。奪うには現実世界で「盗む」という行動を起こさなければならず、攻撃者が姿を現すリスクがあることが抑止力になるからです。

### 1.11 パスワード情報をクラウドで保管する善し悪し

パスワード管理アプリや、同様の機能を持つソフト▶用語集 P.198 には「ク

ラウド連携機能」やクラウド▶用語集 P.195 を用いた「バックアップ機能」があり、これを利用すると複数端末でパスワード情報を共有できたり、明示的にバックアップ処理をしなくても自動でクラウド上にバックアップデータが作られたりします。

この機能が無条件で推奨しない理由は、「重要な情報が複数箇所に存在すれば、流出する可能性がその分増える」からです。

加えて、クラウドサービスを利用する場合、他人の手元でデータが保管されますが、利用者には、そのサービスが運用しているシステムのセキュリティレベルの実態を知ることすら管理することもできません。








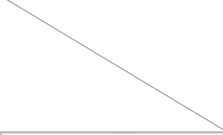

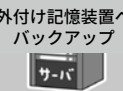


また、パスワード管理アプリのデータがスマホ上にある限りは「PIN コード」方式で守られますが、クラウドのバックアップデータが流出すれば、マシンパワーにものをいわせた高速なオフライン攻撃、暗号化解除の攻撃が可能になるからです。

銀行の口座からお金が盗まれれば、自分にミスがない限り銀行が補填してくれますが、クラウドから流出した情報は実質的に回収不可能です。これは、「お金は補填が可能だが、重要情報の秘密性は戻らない」からなのです。

### 1.12 ノートやスマホを失くした場合のリカバリ考察

さて、パスワードを記録したスマホも紙のノートも、紛失してしまうと困るのは同じです。ただ、スマホの場合、パソコンでスマホのデータを丸ごと暗号化してバックアップをしておけば、紛失しても代替機をパソコンに接続し「復元」を指示するだけで、環境やパスワード管理アプリ

## パスワード管理方法のメリットデメリット

	盗難・紛失 対策	ネット経由の セキュリティ	データの 管理者
 紙のノート	 持ち歩かず自宅などの安全な場所に保管する	 攻撃不可	本人
 スマホアプリ	 盗難・紛失のリスクが高め。バックアップが必要	 セキュリティレベルによる	本人
 外付けHDDへバックアップ		 ただし普段は接続しない	本人
 外付け記憶装置へバックアップ  クラウドサーバにバックアップ		 サービス側のセキュリティレベルによる	事業者

パスワードの管理方法とバックアップ方法を、1つの表で同列にまとめていますが、一番右列のデータの管理者の項目をよく見て下さい。クラウドサービスを使ったバックアップは便利ではありますが、データの管理者は自分ではなくなります。また、クラウドサービスのセキュリティがどのレベルなのかは、自分では容易に判断できません。

パスワードに関してのみは多少の不便さはあっても、自らの責任において管理するのか、それとも他人の手を借りるのか、クラウドはそれに伴うメリットとデメリットをよく勘案して利用しましょう。



の内容を含めて、すべて元の状態にできるものもあります。

また、スマホを丸ごとバックアップしなくても、パスワード管理アプリのデータを、パソコン経由で暗号化された外部記憶装置などにバックアップし、普段は接続せず適切に保管しておけば、復旧は容易です。アプリによっては紙に印刷して保管する機能もあります。

なお、クラウドサービスのメリットとデメリットを理解した上で、クラウドを使った複数機種での連携機能、自動バックアップやそれに付随するリカバリ機能を利用するのは1つの選択肢といえます。

紙のノートの場合は、原則自宅など安全な場所で保管し、持ち運ぶのは避けましょう。万一の盗難などに備え予備を用意しておくとともに安心です。

### 1.13 注意すべきソーシャルログイン

機器やウェブサービスの「ログインパスワード」は、使い回しをしないのが絶対です。しかし、膨大な数のパスワードを暗記するのは非現実的なので、必然的にパスワード管理アプリやパスワード管理のノートを使う必要があります。

この手間は、情報漏えい対策のために「パソコンのウェブブラウザにIDやパスワードを覚えさせる機能(=自動入力)」を使わないならなおさらです。

これを解決する策として、「ソーシャルログイン」▶用語集 P.198 という方法が用いられて来ました。これは、IDとパスワードの管理がしっかりしたウェブサービスのアカウントで、他のウェブサービスにログインして

利用するというものです。

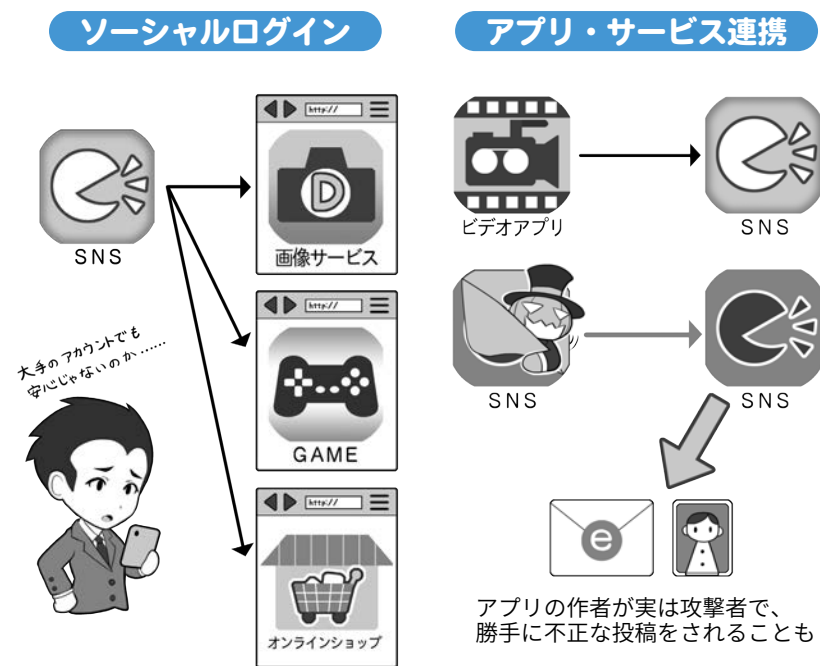
しかし、グローバルで展開しているSNSサービスですら、ソーシャルログインで用いられる身分証明の証(トークン)が流出する事例はあるため、本書では、ソーシャルログインを非推奨として、基本的にそれぞれのサービスは別々のIDとパスワード

を設定することのみを推奨することとします。

トークンが流出すると、IDとパスワードが流出しなくても、ソーシャルログインを設定していたサービスに根こそぎアクセスしてしまえる可能性がありますからです。

一方、それぞれのウェブサービス

## ソーシャルログインとサービス・アプリ連携の違い



ソーシャルログインは、堅牢なサービスのアカウントを別のサービスの鍵に使い便利ですが、大本のアカウントの認証情報が漏れる事案が発生したため、それぞれのサービスに別々のパスワードを使用する基本対応を推奨します。

## アプリなどの連携は定期的に棚卸ししよう



自分が意識的に連携をしていなくても、ネット経由で回ってきた「面白いアプリ」を利用したら、いつの間にか連携されていたということもあります。また、そのときは問題がなくても更新時に権限の拡張を求めてきて、結果的に個人情報を「合法的に」奪うアプリも存在しています。

アプリ連携▶用語集 P.194 やアプリの権限は、定期的に棚卸をして、不必要なものや不審なものは連携解除するか、削除するようにしましょう。

を利用するときに、別々のIDとパスワードを入力する手間を省くために、パスワード管理アプリが進化し、ウェブサービスやアプリのログイン時に、自動的に入力してくれる機能も登場してきました。二要素以上の多要素認証などの使い捨てパスワード▶用語集 P.199 入力も楽になっています。

それらを活用し、パスワードの使い回しをせず、ストレスなくルールを守るようにしましょう。

### 1.14 権限を与えるサービス連携にも注意

ソーシャルログインと混同されやすいものに、SNS▶用語集 P.192 に関する機能で「サービス・アプリ連携」▶用語集 P.196 というものがあります。

例えば、AというSNSにBというサービスやアプリから、投稿を認めるといったものです。具体例としては特徴的な機能を持つカメラアプリにSNSへの写真付き投稿を認めるといったものがあります。

これは、ソーシャルログインとは別の機能ですが、ときに「連携するアプリやサービスに投稿を認める(=権限を与える)」という部分が、攻撃者による攻撃の手段として利用されることもあり、また実際にメールアドレスや氏名が流出した例も存在しますので、利用する場合は気を付けましょう。

また、SNSを利用していると、自分が意識しないうちに誤操作をし、知らずにサービス・アプリ連携していることもあります。

定期的に使用しているSNSアカウントの「連携を確認できる画面」を開いて、知らないアプリや止むを得ず使ったサービス・アプリの連携があれば解除しましょう。

## コラム.1 暗号化の超簡単説明

暗号化とは、自分と相手だけが読めて他人は読めないという、セキュリティを保つ技術です。

暗号化というと非常に難しく感じるかも知れませんが、大丈夫、その心配にはあたりません。

ただ、暗号化の内容を詳しく書くとそれだけで本になってしまうので、ここではその概念だけをごく簡単に説明します。

1. 暗号化とは「魔法をかけて手紙などの内容を読めないようにすること」です。
2. 暗号化の魔法にはいくつもの系統(方式)があり、魔法をかけるには呪文(「暗号キー」)を決めて使います。
3. 魔法の呪文(「暗号キー」)がばれると、魔法が解けて内容が読めてしまいます。
4. 古い系統の魔法の中には、

その仕組みに不備があり、呪文が分からなくても解けてしまうものがあります。

初歩としては、このぐらいの理解があれば大丈夫です。

使用する暗号化方式▶用語集 P.194 が安全かどうかは、魔法研究の専門家に任せましょう。車がどうやって動くのか知らなくても、安全な利用ができるのと同じです。

大切なのは、正しい使用法を知ることと、専門家が「危険が発生した!」という情報を発信したらキャッチし、迅速に避けるように行動することです。

右のイラストでは、具体的に危険が発生する例を描いていますので、是非覚えておいてください。

まず第一歩は、「正しく使うこと」からです。

### Cipher Disk(シーザー暗号)



最も原始的な暗号は、シーザー暗号といわれるものです。文字をずらして記述するだけのシンプルなもの、仕組みさえ分かればアルファベットなら26回試すまでに暗号が解けてしまいます。

上の図は、その暗号を解きやすくするための Cipher Disk (暗号円盤) です。現代の暗号は複雑な演算を伴うために、人力での解読はほぼ不可能です。

## 暗号化ってなに？

### 平文での通信は読めてしまう



暗号化していないと、攻撃者はどこでも盗んで読み放題

## 暗号が破られる場合

### 暗号化方法の種類はいろいろ



シーザー暗号化方法  
× 古い、危険すぎ

「WEP」方法  
× 解読されるからだめ

「WPA」方法  
○ 呪文が長ければ安全

### 暗号化の魔法は内容を読めなくする



※1：暗号化方式 ※2：「暗号キー」

### 暗号破られる例① 呪文がバレている！



### 暗号化したものを送れば攻撃者が読めない



※ただし、攻撃者が「シーザー暗号」を読めない場合

### 暗号破られる例② 方法が古くて解読可能！



### 事前に決めておいた方法(暗号化方法)と呪文(「暗号キー」)で暗号文を復元(復号)する



### 暗号破られる例③ 呪文が簡単すぎて解読される





## コラム.2 パスワードの管理と流出チェックについて

ここでは、パスワードの管理に関する最新の動向を踏まえて、本文でも紹介したテクニックを詳しく解説しましょう。攻撃者から身を守るためには、最新の技術で先手を打つのも1つの対策だからです。

個人情報の流出、と聞くと2021年にグローバルに展開するSNSサービスユーザーの個人情報流出が記憶に新しいです。このような流出事例は、小規模なものも含めると世界中で毎日のように生じており、事例を取り上げれば枚挙にいとまがありません。こうして流出したIDとパスワードは、必ずといってよいほど不正アクセスに使われます。そういった攻撃から身を守るには手段は2つ。1つは、流出しても被害を最小限にとどめるため、サービス毎に別々の長くて複雑なパスワードを設定すること。もう1つはそもそもパスワードを盗めないようにすることです。

### ■パスワード管理アプリの高度な利用

パスワードに関して、NISC▶用語集P.191では、「人は必ずヒューマンエラーを起こす」ことを前提に対処方法を考えます。例えば、パスワードの管理は数が多くなるほど覚えにくく、使い回しをせずサービス毎に別々のものを考えるのは面倒で、ユーザーに厳格な運用を強要するとそのうちワンパターン化したり、同じ物の使い回しが起きたりするのではないかと考えます。

これを解決する方法として、総合的にパスワードを管理する、スマホの「パスワード管理アプリ」などの利用も有効です。パスワード管理アプリは、単にパスワードを保管してくれるだけではなく、条件を設定するとそれに合わせた長くて複雑なパスワードを自動的に生成してくれる他、最近では、ウェブブラウザでのサービスログイン時に、自動的に起動してIDとパスワードを入力したり、アプリ起動時にもIDとパスワードを入力してくれたりするように進化しているものもあります。パスワードを、いちいち管理アプリを見て入力したり、カット＆ペーストしたりする手間も省きつつ、みなさんの負担を軽減する傾向にあるのです。

また、パスワード管理アプリの中には多要素認証で利用する使い捨てパスワードを発生するためのQRコードを、アプリ内に読み込めるようになっているものもあります。このようなQRコードを読み込ませておけば、パスワード管理アプリがサービスごとの「ソフトウェアトークンアプリ」の代わりとして機能してくれるので、サービスごとにアプリを入れることなく、一括して管理できるため便利です。

### ■紙のノートによるパスワード管理の利点と注意点

パスワード管理アプリは利便性に優れていますが、端末がネットに接続している限りサイバー攻撃のリスクからは逃れられません。

一方、紙のノートによる管理は、ネットから遮断されているためサイバー攻撃でパスワードを盗み見ることは不可能です。

注意事項として紙のノートは紛失した場合、中を見られなくする制限はかけられないこと、また、外出時に覗き見されるなどのリスクがあるため、ノートは持ち歩かずに自宅など安全な場所で保管・管理しましょう。万が一、ノートを紛失したり、誰かに覗き見られた可能性がある場合は早急にパスワードを変更しましょう。

なお、記録するパスワードは「実際は含まれない余分な文字を混ぜる」「実際は前後に2,3桁程度、暗記できる数の文字が追加されたものにする」などのさらなる工夫をしておけば、ノートの中身を盗み見られてしまった途端に悪用されてしまう可能性を少しでも下げられるので、より安全なパスワードの保管ができます。

### ■パスワードを無くすFIDO

主としてパスワードが流出するのは、サービス側で保管しているIDとパスワードを含めた個人情報が、多量にまとめて盗まれるケースです。したがって、サービス側に盗むべきパスワードがない場合は、この攻撃は成功しません。そのためにパスワードそのものを無くすことを目指すのがFIDOアライアンス(Googleやマイクロソフト、NTTドコモといったIT企業や通信会社、信販会社、通販会社などが加盟)が進めるFIDOという方法です。この方法では、



利用者が「本人」とあるという認証をパソコンやスマホなどそれぞれの機器の上で行い、利用するサービスへは「本人だと認証しました」という情報のみをやりとりするのです。本人だと認証する方法は、USBセキュリティキー、指紋や顔認証などの生体認証です。

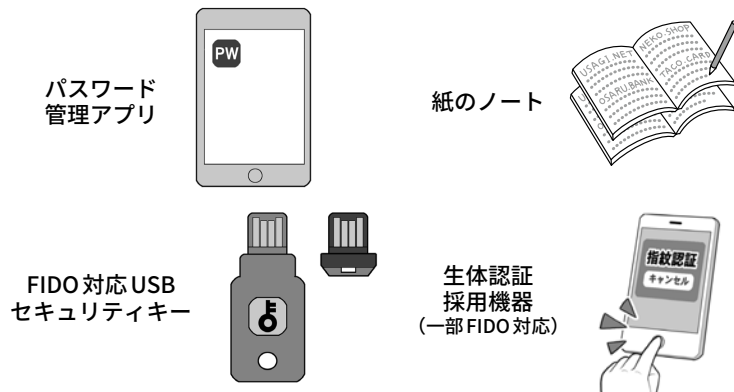
2022年12月にはFIDOアライアンスよりApple、Google、マイクロソフトなどのグローバルIT企業がFIDOの技術仕様を活用した「パスキー」というパスワードを使用しない認証方法を採用することが発表され、今後の普及が期待されています。パスキー対応のサイトやサービスは現状多くはないので、本格的な普及にはまだ時間を要するとは思われますが、グローバルIT企業の本格的採用によりFIDOの利用が大きく進展する可能性は高まったといえるでしょう。

## ■パスワード流出を能動的に検知する

パスワードの流出は、登録しているサービス側から流出の事実が通知される他にも、流出情報の検索サイトを利用すれば能動的に調べられます。

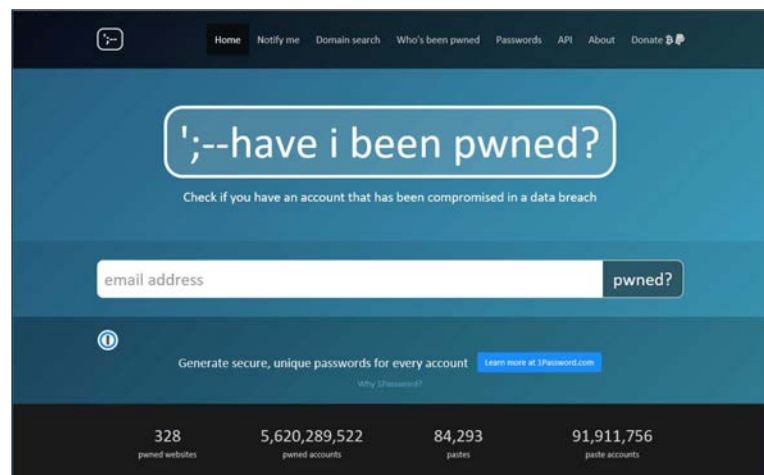
セキュリティ識者のトロイ・ハントさんが、流出したIDとパスワード情報を収集し検索できるようにした「Have I Been Pwned?」は、個人でもウェブサイトで自分のIDとパスワードが過去に流出していないかチェックできる他、アドレスを事前に登録しておくことで流出時に警告のメールが送られて

## パスワード管理と認証の方法



パスワード管理アプリや、FIDO対応機器。これらの導入がセキュリティの向上に役立ちます。またネット接続しない紙のノートによるパスワード管理も、紛失・盗難に備えた上なら安全性は高いといえます。

## 流出IDとパスワードチェックサイト「Have I Been Pwned?」(私、漏えいしてる?)



メールアドレス流出チェックURL: <https://haveibeenpwned.com/>  
パスワード流出チェックURL: <https://haveibeenpwned.com/Passwords/>

他にもFirefox Monitorなどで、同等の機能が提供されています。実績もありセキュリティ業界において評価は高いですが、あくまでも民間のサービスなので、その点を理解して利用しましょう。

きます。

また、パスワードを入力して、そのパスワードが「流出した履歴あり」となった場合、それは、あなたの情報の流出であっても他の人の情報の流出であっても、以降パスワードリスト攻撃の対象になるので変更しておきましょう。

根っことは同じデータベースを用いますが、ウェブブラウザを

提供しているFirefoxもFirefox Monitorとして同様のサービスを提供している他、パスワード管理アプリでもパスワードの安全性チェックに採用する動きが見られます。今後こういった流出情報のチェックサービスは増えていくと予測されるので積極的に活用して、攻撃される前に対処するようにしましょう。

### コラム.3 パスワードを記録する演習

前項でも解説しましたが、パスワード管理アプリは利便性に優れていますが、端末がネットに接続している限りサイバー攻撃のリスクからは逃れられません。一方、紙のノートによる管理は、ネットから遮断されているためサイバー攻撃でパスワードを盗み見ることは不可能です。

加えて、P.78「コラム.6 デジタル遺産相続」で説明したように、大切な家族のためにパスワードなどを記録しておくことは重要です。

次頁のメモ欄を利用しながら、安全にパスワードを記録・保管する方法を実践してみましょう。

注意事項として紙のノートは紛失した場合、中を見られなくなる制限はかけられません。また、外出時は覗き見のリスクがあるため、ノートはむやみに持ち歩かずに自宅など安全な場所で保管・管理しましょう。

万が一、ノートを紛失したり、誰かに覗き見されたりした可能性がある場合は、予備を作成・保管しておき、その予備を参考にしながら早急にパスワードを変更することが必要です。

また、パスワードを記録する際には、盗み見した者が記録されたパスワードを使用して、すぐに悪

用できてしまう可能性を少しでも下げる工夫を施しておく、より安全にパスワードを保管できます。

具体的には「実際には含まれない余分な文字を混ぜてノートに記録する」「実際のパスワードは前後どちらかに2,3桁程度、暗記できる数の文字が追加されたものに設定して、すべての文字はノートに書き残さない」などがあります。工夫次第でさまざまな方法が考えられますし、煩わしさを感じない、無理のない範囲で工夫してみましょう。

#### パスワードを紙のノートに記録しておくことは重要

##### パスワードを確認できて便利で、万一の備えとしても家族のために役立つ

サイト名：通販〇〇	サイト名：動画サイト〇〇	課金しているサービスはプラン名や金額を記載しておくとい
ID/ユーザー名：niscstaro	ID/ユーザー名：nischanako	
パスワード：3%2/aGNA%G!Listw	パスワード：Dc(fq--a)+d4un%	
メールアドレス：nin*****@gmail.com	メールアドレス：hn*****@gmail.com	
メモ：毎月5の付く日がお得！	メモ：サブスクプラン利用(月額980円)	

##### 盗み見されてもすぐに悪用されないような工夫があるとより安全

サイト名：	サイト名：	パスワードのみなど、最低限の情報の記録に留める
ID/ユーザー名：	ID/ユーザー名：	
パスワード：X!#KejNiD9\$+Z7JT,qRl/_hs!	パスワード：TnW\$TMAFyWXPqAhzRKEIY72s9	
メールアドレス：	メールアドレス：	実際は前後どちらかに2,3桁程度、暗記できる数の文字が追加されたパスワードに設定して、すべての文字はノートに書き残さない
メモ：実際のパスワードは偶数番号だけの文字にする	メモ：	

サイト名：

ID／ユーザー名：

パスワード：

メールアドレス：

メモ：

サイト名：

ID／ユーザー名：

パスワード：

メールアドレス：

メモ：

サイト名：

ID／ユーザー名：

パスワード：

メールアドレス：

メモ：

サイト名：

ID／ユーザー名：

パスワード：

メールアドレス：

メモ：

サイト名：

ID／ユーザー名：

パスワード：

メールアドレス：

メモ：

サイト名：

ID／ユーザー名：

パスワード：

メールアドレス：

メモ：

サイト名：

ID／ユーザー名：

パスワード：

メールアドレス：

メモ：

サイト名：

ID／ユーザー名：

パスワード：

メールアドレス：

メモ：

# 安全な無線LANの利用を支える暗号化について学ぼう

私たちが日常的にインターネットで送信するIDやパスワード、送受信するメールの内容や添付ファイル、ウェブサイトで閲覧する内容は、常に攻撃者の盗聴や盗み見の危険にさらされています。

攻撃者はそうした情報を不正に入手して売却したり、さまざまな手段を駆使して直接お金を手に入れるために利用したりします。これを阻止するためには、通信している情報の暗号化が必要となります。

そもそもインターネットは、その始まりにおいて暗号化などが全くされておらず、情報をそのままの状態(平文)で送受信するシステムでした。

インターネットは、蜘蛛の巣状に接続し合ったサーバ間で、どこかの経路が遮断されても迂回して通信を続ける、そういう面では先進的ではあったのですが、攻撃者などの悪意の存在を前提に構築されてはいなかったからです。

その後、インターネットの発展にしたがって、世の常として悪意を持ったものたちが現れ、コンピュータウイルスの開発や、パスワードを破って侵入しての情報の奪取、通信中の情報の盗聴が行われるようになり、それぞれ対策が必要になりました。

コンピュータウイルスにはウイルス対策ソフトが、パスワード破りには複雑なパスワードや多要素認証などが、そして通信中の情報の盗聴には暗号化が、攻撃者への防御として普及していくわけです。

## 2.1 それぞれの状況に合わせた暗号化の必要性

一口に通信の暗号化といっても、さまざまな状況に合わせた、それぞれの暗号化があります。

私たちが通信すること1つをとっても、有線LAN、LTE▶用語集 P.191などの携帯電話回線、Wi-Fiなどの無線LANなど、多様な通信手段があります。

このうち攻撃者にとって、手軽に行いやすい攻撃対象の1つとして無線LAN通信の盗聴があります。

無線LANではその名のとおり通信機器が無線(電波)を使って通信するので、盗聴に際してとくになにか物理的な工作をする必要はありません。通信が暗号化されていないか、無線LANに対応したパソコンを持って電波が届く範囲に居るだけで、簡単に盗聴することが可能です。

なお、有線通信も暗号化されていなければ、通信経路上のどこかで情報を盗聴することが可能です。

さらに、攻撃者が利用者のふりをしてメールサーバやパソコンに侵入すれば、中にたまったメールや、内蔵記憶装置などの中の情報も盗み見し放題です。

パソコンがマルウェアに感染して、記憶装置の中の暗号化されていないファイルが流出し、インターネット上に投稿されたあげく、世界中から見放題になるという事件もありました。

そういった状況を避けるためには、仮に盗聴されたり、侵入されたり、

流出してしまっても、通信内容や重要なファイルの中身が見られないように、それぞれのシーンに応じた適切な暗号化をする必要があります。

その対策をつぶさに挙げていくと数限りないのですが、このセクションでは、まず私たちの生活で最も身近な無線LAN通信の暗号化について説明しましょう。

## 2.2 無線LAN通信(Wi-Fi)の構成要素

インターネットにつながった無線LANアクセスポイント▶用語集 P.203さえあれば、いちいちIT機器にLANケーブルをつながなくても、手軽にインターネットを利用できる、無線LAN(Wi-Fi)による通信。

会社で利用する無線LANでも、外出時に利用する公衆無線LAN▶用語集 P.196でも、セキュリティがしっかりしていなければ、通信中に送信したIDやパスワード、データすべてを攻撃者に盗まれる危険性があります。

それを理解するために、まずは無線LAN通信を構成する要素を知っておきましょう。

最初は無線LAN通信を提供する「無線LANアクセスポイント」になる機器。一般には「無線LANアクセスルータ」▶用語集 P.203「Wi-Fiルータ」▶用語集 P.193あるいはシンプルに「ルータ」などと呼ばれます。

この機器で無線LAN通信を提供する際、最低限以下の3つを設定します。



- ①識別名「SSID (Service Set Identifier)」▶用語集 P.192
- ②通信内容を暗号化するための「暗号化方式」
- ③その暗号化のための鍵となる「暗号キー」(設定上は暗号化キーと書かれる)

「暗号キー」は利用者が無線 LAN アクセスポイントに接続するときのパスワードのように使われる他、通信内容を暗号化するときと、元に戻す復号(元の平文に戻す)のときの鍵として使われます。

ここまでが無線 LAN アクセスポイントの構成要素です。

スマホやパソコンが無線 LAN を利用して通信するときは、利用する機器の無線 LAN (Wi-Fi) 設定で、SSID を手掛かりに目的の無線 LAN アクセスポイントを見つけ、必要な場合は暗号化方式を選択し、「暗号キー」を入力して接続します。

なお、災害時や公益目的で、誰でも無線 LAN を利用できることを目的として、「00000JAPAN」のように「暗号化無し」で提供されている無線 LAN アクセスポイントもあります。(その安全性は別として)

この場合は利用時に暗号化方式の設定も「暗号キー」も必要ありません。

次に無線 LAN の危険要素について説明します。危険なポイントは以下の2つになります。

- ①「通信が暗号化されていないか、されていても安全ではない場合」
- ②「暗号化の鍵(「暗号キー」)が公開か漏れている場合」

## それぞれの状況に合わせた暗号化

### 通信の暗号化

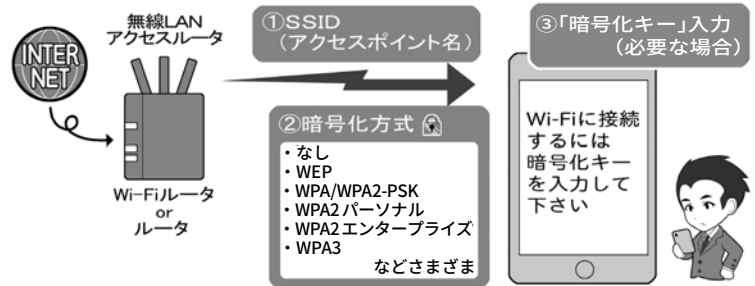


### ファイルの暗号化



暗号化には、電話、メール、ウェブサイト閲覧などの「通信の暗号化」と、ファイルやパソコンの内部記憶装置などの「ファイルの暗号化」があります。

## 暗号を使う無線 LAN の構成要素



暗号化を伴う無線 LAN 通信には暗号化方式と「暗号キー」の設定が必要となります。「暗号キー」は機器に接続するときパスワードのように使われます。

## 公衆無線 LAN が安全とは限らない

プロバイダ▶用語集 P.202 か  
携帯電話キャリア



- SSID: MUSENLAN1  
暗号化無し or  
暗号方法読済み ×
- SSID: MUSENLAN2  
「暗号キー」を  
他人と共有 ×
- SSID: MUSENLAN3  
「暗号キー」が利用者  
ごとで異なる ○



信頼がおける企業や団体でも、提供している公衆無線 LAN が安全とは限りません。アクセスの利便性のため暗号化無しで提供される場合もあるからです。

## 「暗号キー」共有は接続しちゃダメ



暗号化方式が安全でも、「暗号キー」を見知らぬ他人と共用するのは、すべて危険です。

こういった方式は、公衆無線 LAN やホテル、公共機関、インターネットカフェやレストランなどで広く使われています。

提供する側が善意で行っていても、攻撃者は善意で行動しません。攻撃できる環境があると判断するだけです。

安全な通信をするために、自前で暗号化を行うテクニックがなければ利用してはいけません。

## 2.3 暗号化無しや、方式が安全ではないものは危険

無線 LAN の利用において、通信が暗号化されていないものは、内容が平文で送受信されているので、なんらかの別の手段での暗号化を行わないまま使っていると、攻撃者に盗聴され、即座に内容を知られてしまいます。

そのため、まず「暗号化無し」のアクセスポイントは基本的には利用しないようにしましょう。

災害時など例外的に使用する場合は、後述の「10 公衆無線 LAN が安全でない場合の利用方法」を参照してください。安全な利用には最低限、別の手段での暗号化が必要だと覚えておいてください。

暗号化無しの通信は、例えるなら拡声器を使って遠くの人と話しているようなもので、耳を傾ければその場にいる誰もが内容を知ることができるのです。

また、無線 LAN 通信が暗号化されていても、その暗号化方式がすでに破られていて安全ではない場合、上記と同様に攻撃者は通信を盗聴して、内容を解読することができるので、これも危険です。使用しないようにしましょう。

これは、「英語でしゃべればわからないだろう」と思ったら、周りに居た人も英語が理解できて、内容がばれるイメージです。

危険である暗号化方式の具体例としては、「WEP」▶用語集 P.193 という名前のもや、方式の名称の中に「TKIP」▶用語集 P.192 と含まれるものが該当します。

一方、暗号化方式として安全とされるのは WPA ▶用語集 P.193-PSK (AES ▶用語集 P.190)、WPA2 ▶用語集 P.193-PSK

(AES)、WPA2-EAP、WPA2-エンタープライズ、IEEE 802.1x、SIM 認証▶用語集 P.192、そして無線 LAN の多くの問題点を解決するために登場しつつある WPA3 ▶用語集 P.193、それらの記述があるものです。安全な方式の詳細は P.129 を参照してください。

## 2.4 暗号化方式が安全でも「暗号キー」が漏れれば危険

暗号化の方式自体が安全でも、通信を暗号化するための「暗号キー」が漏れていると、通信を盗聴した攻撃者が通信内容を復号したり、同じ SSID と「暗号キー」を使って偽の無線 LAN アクセスポイントを作り、本物のアクセスポイントになりすまして通信内容を根こそぎ奪う、中間者 (Man-in-the-middle) 攻撃を行ったりすることができるようになります。

イメージとしては、破られていない暗号化方式は誰も知らない言語で、「暗号キー」が辞書。しかし、辞書が他人の手に渡っていると、たとえ知られていない言語でも解読されてしまうし、その情報をもとに通信する相手になりすますこともできる、というものです。

この至極単純な「暗号キーが漏れていれば、暗号化された通信を復号し解読できる」ということも、よく覚えておいてください。

## 2.5 会社などでの安全な無線 LAN の設定 (暗号化方式)

会社などで無線 LAN を使用する場合、先ほど説明した安全な暗号化方式である WPA-PSK (AES) か WPA2-PSK (AES)、WPA3 を利用し、「暗号キー」を基準にしたがって、完全にランダムで十分に長くして、さらに

その「暗号キー」を「社員や会員だけが知っている」状態に保てれば、ほぼ安全に使用することができます。

これを実現するため、無線 LAN 機器設置時には、まず機器を購入したときの初期の「暗号キー」は変更しましょう。上記のとおり「暗号キー」は関係者だけしか知らないものに変更しなければ安全が確保できません。

メーカーによっては「暗号キー」が同一機種で共通だったり、付け方に規則性があるかもしれないからです。

極端な考え方をすれば、その機種がメーカーから手元につくまでに、初期の「暗号キー」を見たものがないともいい切れません。

なお、無線 LAN アクセスポイントの名前となる SSID を変更する場合、会社や団体の名前、社員や会員個人々人を想起させる語句は使わないようにしましょう。会社や団体、もしくはあなたが攻撃の対象の場合、攻撃すべき無線 LAN が特定されるヒントになるからです。

小さい会社などで使う家庭用無線 LAN アクセスルータは、標準で 2 つ以上の SSID を持てるものが多く、そのうちの 1 つには、WEP などのものは安全でない古い暗号化方式が設定されている場合があります。これは、主に古いゲーム機などが接続できるようにするためだったりします。

しかし、こういった設定はセキュリティ上の穴となるので、設定を変更し安全な暗号化方式にするか、安全でない暗号化方式の設定のものはすっぱりと停止しましょう。接続する古い機器が、安全でない昔の暗号化方式しか選べない場合は、利用を諦め買い換えましょう。

同様に、来客用に簡便な「暗号キー」や、問題のある暗号化方式を使った接続設定があれば、これも停

止しましょう。

来客に社内用のSSIDに接続させるのも安全ではありません。「暗号キー」が「社員・会員だけが知っている状態」では無くなってしまいます。どうしても来客用に一時的にアクセスポイントを開放したい場合は、2つのSSIDの1つを来客専用にし、2つのアクセスポイント▶用語集 P.193の間で、お互いのアクセスポイントに接続した機器が見えないような分離状態に設定してから提供しましょう。そして来客が帰宅したら、そのSSIDは利用停止しましょう。

## 2.6 会社などでの安全な無線LANの設定(その他)

無線LANアクセッスルータには、ウェブブラウザを使って本体の設定画面にアクセスするための、機器管理用のIDやパスワードがあります。それは管理者アカウントとも呼ばれます。こちらのパスワードも必ず購入時のものから変更しましょう。このパスワードはログイン画面から使用するものであり、「ログインパスワード」の基準に従い変更しましょう。

この設定画面が、もし家の中からだけでなくインターネット側からアクセスできるようになっていたら、アクセスできないように変更しましょう。

設定画面は無線LANで接続した機器からアクセスできず、有線LANからのみアクセスできる設定にしましょう。この設定をする理由は、家の外にいる攻撃者が姿を隠した上で無線LANに接続し、設定内容を変更したりしてしまわないようにするための予防策です。

無線LANアクセッスルータにルータ本体と機器のボタンを押すだけで

## 会社内での無線LANの利用

### ①出荷時の管理者パスワード、「暗号キー」の変更



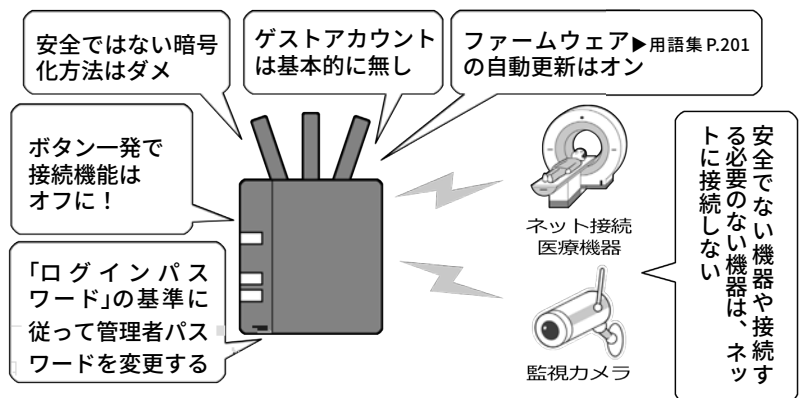
出荷された機器は、厳密に言えば誰かの手によって梱包されているので、出荷時の「暗号キー」が見られている可能性があります。必ず変更しましょう。

### ②「暗号キー」は社員・会員だけの秘密



家庭で使える暗号化方式は、「暗号キー」を社員・会員のみの秘密にすることが、安全に使うための絶対条件です。部外者には教えないようにしましょう。

### ③ルータと機器の安全な運用



会社や団体で無線LANや有線LANを使用する場合、注意したり設定を変えたりしなければならない点がたくさんあります。必ずチェックして安全な状態を作りましょう。また、基本的に接続する必要がない機器を、むやみにLANに接続しないようにしましょう。

簡単に接続できる「WPS」「AOSS」「無線LANらくらくスタート」といった名称のもの、もしくは類似の機能がある場合は利用不可にしましょう。この設定をオンにしていると、目を

離したすきに、利用してほしくない来訪者が、ボタン一発で手元の機器を無線LANに接続できてしまうからです。

どうしても利用する場合は、設定



画面からそのときだけオンにして使用し、設定後はオフに戻しておきましょう。

UPnP(Universal Plug and Play)▶用語集 P.193 の設定も、不用意に社内の LAN の機器をインターネット上に公開してしまう可能性があるためオフにします。そしてネットに接続する必要のない機器は、無線・有線にかかわらず、そもそも LAN に接続しないようにしましょう。

無線 LAN アクセスルータの設定画面に、本体ファームウェアの自動アップデート▶用語集 P.194 機能がある場合はオンにしておきましょう。それによりメーカーがルータの不具合(バグ)などを修正した場合、自動で更新が行われセキュリティが最新に保たれます。もし自動アップデートの設定がない場合は、自分のスマホに定期的なアラームを作り、それにしたがってファームウェアが更新されていないかチェックし、公開されていれば更新処理を行いましょう。

なお、昔に書かれたセキュリティの解説記事によっては、「SSID を隠すステルス設定」や、接続できる機器を LAN 機器の番号で制限する「MAC アドレス規制」を対策として推奨していたりします。

しかし、ステルスになった SSID も簡単に探し出すことが可能ですし、MAC アドレスは盗聴可能かつ詐称可能ですので、これらの対策を行っても安全性は向上せず、むしろ利便性が悪くなるので、設定する意味はないでしょう。

無線 LAN アクセスルータは、社内のセキュリティの要です。お使いのルータに上記のようなセキュリティの設定がない場合や、安全な暗号化方式の設定がない古い機器の場合は、速やかに利用を停止し最新のものに

買い換えるようにしましょう。また、どうしてもマルウェア感染が心配な場合は、「am I infected?」(<https://amii.ynu.codes/>) というサービスを利用すれば、現在使用中の機器が感染しているかどうかの確認ができます。積極的に試して安全性を確認しましょう。

## 2.7 公衆無線 LAN 利用時の注意

公衆無線 LAN の安全な利用は、社内・団体内用の無線 LAN の安全な利用と少し事情が異なります。

例えば公衆無線 LAN で「WPA-PSK (AES)/WPA2-PSK (AES)」の方式の無線 LAN が提供されていた場合、暗号化方式自体は安全でも、別の危険があります。

上記の名称の中の PSK の部分は Pre-Shared Key の略です。利用にあたり「暗号キー」を事前に共有する方式のことで、この方式では社内などの利用と同様に、複数の人が同じ「暗号キー」を使うことになります。これを公衆無線 LAN にあてはめると、全く知らない人と、同じ「暗号キー」を一緒に使うことになるわけです。

その設定の状態で無線 LAN 通信を行うと、「暗号キー」を知っている攻撃者により、通信内容を直接盗聴されたり、なりすまし無線 LAN アクセスポイント(偽アクセスポイント)を使った攻撃をしかけられ、盗聴される可能性を避けられません。

しかし、この方式を含め安全でない暗号化方式は、街中のカフェやレストラン、ホテル、あるいはインターネットプロバイダや携帯電話キャリアが提供する公衆無線 LAN でも広く使用されています。これらのアクセスポイントはすべて潜在的に危険と

いうことになります。

こういった危険なアクセスポイントを使用する場合、無線 LAN 通信の暗号化とは別の暗号化機能で対処する方法があります。それについては後述します。一方、安全な暗号化方式の選択で安全性を確保する方法もあります。

## 2.8 個別の「暗号キー」を用いる方式の公衆無線 LAN

公衆無線 LAN において通信の安全を確保する方法は、危険な暗号化方式などを使わないことは当然として、「暗号キー」を他人と「共有しない」で個別の「暗号キー」を用いる方式を利用することです。

この方法は、公表されている公衆無線 LAN アクセスポイントの情報の中で「WPA2-EAP、WPA2-エンタープライズ、IEEE 802.1x、SIM 認証」といった用語が含まれるものを選択するのです。

携帯電話キャリアなどは、いくつかの異なる暗号化方式の公衆無線 LAN を提供している場合があり、ウェブサイトなどで、それぞれの SSID が採用している暗号化方式が、きちんと掲示されています。

利用前にそのページをチェックし、上記の暗号化方式のキーワードを頼りに、安全な接続ができる公衆無線 LAN の SSID を探してから利用しましょう。

「WPA2-EAP、WPA2-エンタープライズ、IEEE 802.1x、SIM 認証」などが公衆無線 LAN として安全である理由は、これらの方式を採用した無線 LAN アクセスポイントを利用する場合、公衆無線 LAN サービスの提供者が、利用する 1 人 1 人の機器または利用者を識別して個別の認



証を行い、個別の「暗号キー」を用いて通信を行うからです。

そのため、他人と同じSSIDに接続しても、自分用の「暗号キー」を他人に知られることがないのです。

一例を挙げると、「SIM認証」と呼ばれる方式では、それぞれのスマホなどに入っているSIMカードの情報を用いて認証＝接続許可を出すわけです。SIM▶用語集P.192は1枚1枚別々の情報が入っているので、誰かと「暗号キー」が被ることなく安全な通信が確保されるわけです。

## 2.9 公衆無線LANに関して新規に購入したスマホなどで行うこと

新規契約や機種変更、携帯電話会社の乗り換えなどをして、新しいスマホを手に入れたら、まずやるべきことがあります。

そのスマホには、携帯電話キャリアで提供しているさまざまな方式の公衆無線LAN用の自動接続設定が、安全性に関係なくまとめて導入されていることがあるからです。







購入後、細かい設定をしなくても自動的に公衆無線LANに接続できるので便利と思われがちですが、この状態では、意図せず「安全でない方式の公衆無線LAN」に、接続してしまう可能性があります。

新しいスマホなどを手に入れたら、まず接続される可能性があるアクセスポイントの暗号化方式を調べましょう。安全でない公衆無線LANのアクセスポイントに接続してしまった場合、無線LAN接続を切断して、その接続用のプロファイルも削除し、できれば二度とそのアクセスポイントに自動接続されないようにしましょう。

また、知らない公衆無線LANア

## 公衆無線LAN通信の表示の意味

### ①スマホやパソコンの画面から見た無線LAN暗号化

接続	Android	iOS, mac OS	Windows
× (暗号化無し)			
△ (暗号化有り)			

### ②詳細な区分けから見た無線LAN暗号化

接続	ネットワークの種類	暗号化キー (「暗号キー」)	解説
×	暗号化無し	なし	暗号化無しは論外
×	WEP	事前入手	解読済み。使用は不適切
×	WPA-PSK	(TKIP) 事前入手	TKIPには暗号化にセキュリティ上の不安あり。
△	WPAパーソナル	(AES) 事前入手	AESは暗号解読不可能とされているが、「暗号キー」が事前に存在し、利用者は皆同じものを共有するので、暗号解読の可能性あり
×	WPA2-PSK	(TKIP) 事前入手	
△	WPA2パーソナル	(AES) 事前入手	
○	WPA2-EAP *2 WPA2エンタープライズ	(AES)	SIM認証(端末個別)*2 個別のパスワード、クライアント証明書認証▶用語集P.195(利用者個別) SIM認証ではSIMの情報を認証に用い、個別の「暗号キー」が利用されるので通信内容の不正な解読は困難。他にも利用者を個別に認証するEAP-TTLS,EAP-TLSなどの方式もある

上の表は、Android、iOS、macOS、Windowsなどで、無線LANアクセスポイントを選択するときの画面に表示されるアイコンの例になります。それぞれ2種類のアイコンしかありません。そしてこのアイコンは、各アクセスポイントが信頼できるかどうかを表しているのではなく、単純に「暗号化されているかどうか」だけを表しています。

下の表は、暗号化方式のそれぞれの安全性とその理由を書き出したものです。この2つの表を比較すると、すでに暗号化が破られており、利用が推奨されていない「WEP」が、表示アイコン上は暗号化に分類されていることがわかります。アイコンは暗号化の有無を表しているのですが、アイコンは安全性の担保ではないと認識して下さい。Androidは、接続したアクセスポイントをタップすると「セキュリティ」の項目でネットワークの種類の暗号化方式などを確認できます。Windows、macOSは調べるのに手間がかかります。iOSでは簡単に確認する手段がありません。

なお、WPA3が普及すると、これらの問題点のかなりが解消されるようになります。

\*1：Windowsではバージョンによってアイコンに「セキュリティ保護あり」と表示される場合もあります。

\*2：例としてはNTTドコモでアクセスポイントの名称（SSID）が「0001docomo」、auで「au-Wi-Fi2」、ソフトバンクで「0002softbank」のものがWPA2-EAPの方式です。各携帯電話キャリア提供の無線LANアクセスポイントの一部で、自動接続になっているため意識することはありません。その他の安全性が確保されていないと判断したアクセスポイントに接続されている場合は、接続を切ることが推奨されます。

## 自宅や会社のルータが感染状況が確認できる「am I infected?」



「am I infected?」 <https://amii.ynu.codes/>  
家庭や会社のルータやウェブカメラなどのIoT機器を狙ったサイバー攻撃が急増しており、今使用しているルータも感染しているかもしれません。

「am I infected?」は、横浜国立大学 情報・物理セキュリティ研究拠点が運営するマルウェア感染・脆弱性診断サービスで、ルータの感染状況を確認ができます。積極的に試して安全性を確認しましょう。

アクセスポイントなどに勝手に接続されてしまった場合は、切断した上で同様に設定を削除して、以降自動で接続されないようにしましょう。

## 2.10 公衆無線LANが安全ではない場合の利用方法

なお、いつでも安全な状態の公衆無線LANを利用できるとは限りません。先ほど少しだけお話した、観光客用や、災害時に設置される「00000JAPAN」▶用語集 P.190 などの「暗号化無し」の公衆無線LANしか利用できない状況も考えられます。

しかし、「暗号化無し」もしくは「危険な状態」で提供されている無線LANアクセスポイントを不用意に利用すると、攻撃者から見れば獲物が絶好の狩り場に飛び込んできた状況になってしまいます。

対策は、「無線LANの暗号化に頼らず、自前で通信を暗号化して盗聴対策をする」ことです。

以降の手順はややハードルが上がりますので、無理をせず自前の携帯電話回線、もしくはパソコンならばスマホをルータ代わりに利用する「テザリング」▶用語集 P.199 の範囲で、手軽かつ安全にインターネット接続することをおすすめします。しかし、災害時には、そのような環境整備が難しい場合もあるでしょう。

どうしても暗号化無しのネットワークを使わざるを得ないときは、流出して困るような重要情報を送信しない、最低限の使用に留めることを心掛けてください。

## 2.11 自前の暗号化による盗聴対策

自前の暗号化で盗聴対策をする第

一步は、ウェブブラウザでのインターネット閲覧では「https://」から始まるもののみ、メールでは「SSL/TLS」▶用語集 P.192 を使った通信設定になっているもののみ、スマホなどのアプリでは暗号通信でサーバに接続するもののみを使用する方法です。

前者2つに関しては、後ほどそれぞれ詳しく説明します。

スマホアプリに関しては、iOSでは、Appleのアプリ開発者向けガイドによると公式ストアに登録するアプリには基本的にHTTPS通信を強制する「ATS」を有効にすることが求められています。

AndroidではPlayストアのアプリダウンロード画面には通信の暗号化の有無が表示されます。開発者向けブログによると、アプリの通信はHTTPSに限定されているわけではないようですが、通信の暗号化とTLSがほぼ同一視していること示唆する記載があるようです。

しかし、盗聴や情報流出のトラブルがあるものは使用は控え、多くの人が使用しているアプリを使用した方が無難でしょう。

## 2.12 まとめて暗号化するVPN

こういった個別の面倒な対策ではなく、まとめて一気に対策をする方法もあります。それはVPN(Virtual Private Network: 仮想プライベートネットワーク)▶用語集 P.193 の個人利用です。

VPNとは元々は、地理的に離れた2点間をインターネットを利用しながら専用線で接続したかのように接続する技術です。まるで会社内のLANで接続されているように、秘密を守りつつ互いに通信することがで

きます。

VPNはインターネットを使って事業所間を接続してありますが、その通信が外部から盗聴できないように暗号化して秘密を守っているのです。

これを「事業所から事業所」ではなく、「個人のIT機器から安全な場所にある出口サーバ」に置き換えて利用するのが、VPNの個人利用です。

この場合、通信は自分のスマホやパソコンから、少なくとも安全な場所にあるとされる出口サーバまで、無条件ですべて暗号化されるので、どのようなソフトやアプリでも、また、その間の公衆無線LANの暗号化方式が安全でなかったり、そもそも全く暗号化されていなかったりしても、攻撃者に盗聴される心配は少なくなります。

ただ、このVPNの使い方はまだ、一般の利用者が豊富な選択肢の中から選び、ボタン1つで簡単に使える程にはこなれていません。

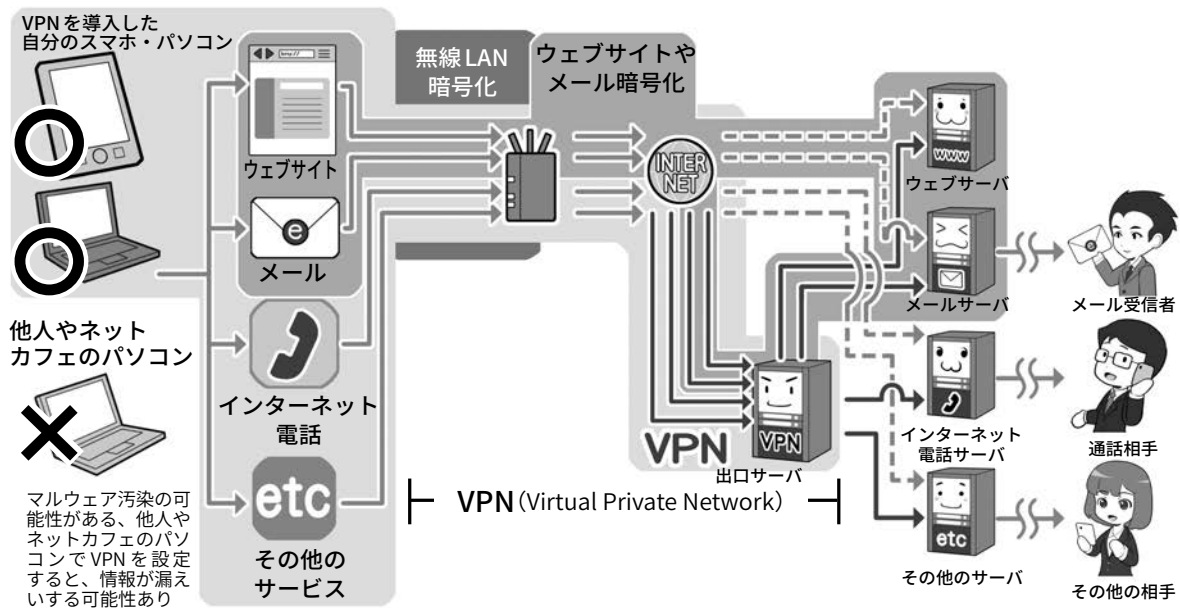
現状は、一部プロバイダが有料サービスで提供していたり、あるいは有料アプリで提供されていたりする程度で、無料で安全性が高く手軽に使えるものは、自分で設定画面を書き換える必要があるなど、導入にスキルが求められます。

利用するVPNのサービスによっては、誤ったアクセスポイントに誘導されたり、VPN接続が切れると暗号化されていない状態に移行して通信を継続したりしてしまうものもあるので注意しましょう。VPNを利用したい場合は、そういった問題点問題を理解したうえで導入するようにしましょう。

なお、VPNが通信を暗号化するのは出口サーバまでであり、その先の通信の暗号化が行われない点は注意が必要です。

## さまざまな場所から安全なアクセスを可能にするVPN

### ① 詳細なVPNのイメージ



VPNを図で説明すると、上のように入り組んでよく分からなくなってしまうので、簡単な図を下に用意しました。くじけそうな方はまず下をご覧ください。

上の図では左から右に向かって通信を行う場合、無線LANの暗号化、ウェブサイトやメールの暗号化、VPNとそれぞれ暗号化の守備範囲があることが分かります。

無線LANの暗号化は範囲が短く、ウェブサイトやメールの暗号化は文字どおり用途が限定されます。VPNはすべての通信を暗号化し、かつ広範囲にカバーしてくれます。

しかし、その範囲は利用者の機器から安全と思われる場所に設定された出口サーバまで限定であり、その先の目的のサーバまでは暗号化されない区間が残ります。VPNさえあればすべて安全というわけではないのです。

### ② 簡単なVPNのイメージ



VPNを簡単なイメージで説明するとこの図のようになります。

スタート地点（自分のパソコンやスマホの中）でデータを護送車に乗せて全部まとめて暗号化、危険地帯を突破し、信頼がおける安全な場所（出口サーバ）に着いたらデータを解放します。

VPNは暗号化されていない無線LANを利用するのにも役に立ちますし、危険性があると思われる通信回線の盗聴、検閲や監視がある国からの安全な通信にも役立ちます。

また、災害時などに利便性を優先して提供される、暗号化無しの公衆無線LANを利用する場合でも役に立ちます。

ただし、そもそもだれが運営しているのかよく分からないような無線LANアクセスポイントには、多分に攻撃者が潜んでいる可能性があるため、攻撃の手段は予測できず、VPNを使えたとしても積極的な利用は推奨しません。



# 安全なウェブサイトの利用を支える暗号化について学ぼう

## 3.1 無線 LAN の暗号化と VPN の守備範囲

ウェブサイトを見るときに、ウェブブラウザ上部のアドレスバーと呼ばれるウェブサイトの住所(URL)▶用語集 P.193 を入れる欄内が①http://で始まっている、②「保護されていない通信」や「安全ではありません」と表示されている、③先頭に注意喚起の🔒や🔒のマークがある場合、その通信は平文で送受信されています。

平文での通信は、通信の途中、攻撃者によっていつでも盗聴や改ざんされ、すべてもしくは一部が偽の情報に書き換えられる可能性があります。そうさせないためには、ウェブサーバ▶用語集 P.194 との通信の暗号化が必要になります。

前項では、通信の暗号化を行うために、無線 LAN 通信の暗号化と、VPN が登場しました。

利用者が目的のウェブサーバなどと通信するとき、無線 LAN 通信の暗号化では、利用者の機器から無線 LAN アクセスポイントまでの、すべての通信が暗号化されます。一方、無線 LAN アクセスポイントから、目的のウェブサーバまでの通信は、無線 LAN 通信ではないので暗号化されません。

一般の利用者向けの VPN サービス(以下VPN)では、利用者の機器からインターネット上の安全な場所にある出口サーバまで、無線であっても有線であってもすべての通信を暗号化します。しかし、出口サーバから目的のウェブサーバまでの通信は

暗号化してくれません。

それぞれの守備範囲には限界があり、したがって攻撃できるポイントが残るわけです。

では、無線 LAN や VPN では暗号化してくれない区間の通信の暗号化や、前項にあった、なんらかの理由で無線 LAN 通信の暗号化や VPN が使えない状況で安全に通信をしたい場合、どのような対処方法があるのでしょうか。

代表的なものとしては、ウェブサイト閲覧やメール送受信、通信をする用途に限定して、利用者のそれぞれのソフトやアプリから目的のサーバまでを個別に暗号化するやり方があります。

## 3.2 すべての通信と、その一部であるウェブサイトとの通信

無線 LAN 通信の暗号化と VPN では、暗号化対象を「すべての通信」と書きましたが、ウェブサイトを閲覧するための通信の暗号化は、その「すべての通信」の中の一部「ウェブサイト閲覧に関する通信」に限定した暗号化になります。

通信には、ウェブサイト閲覧やメール送受信の他に、インターネット電話、一部のアプリや特殊な機器など、目的などに応じて多様な通信が存在します。この多様な通信のことをテレビに例えるなら「テレビで視聴できるすべての電波放送(チャンネル)」と大きくくりになり、ウェブサイトを閲覧する通信は、その中の1つのチャンネルにあたります。そして、

通信にはさまざまなチャンネルが存在する、とすればイメージしやすいでしょうか。

インターネットの通信では、このチャンネルにあたるものを「ポート」▶用語集 P.202 と呼び、ウェブサイトの閲覧の通信は、通常「ポート 80」「80 番ポート」という名称で、文字どおり 80 番のポートで行います。

80 番ポートを使って送受信される通信は、基本的に暗号化されていない平文で、仮にこの状態で ID やパスワード、個人情報などを送信すると、通信を盗聴している攻撃者はとくになんの工夫をしなくても情報を盗むことができます。また、情報が送受信ともに改ざんされたり盗まれたり、偽の情報で取引などをさせられる可能性もあるのです。

それを避けるため、ウェブサイトを安全に閲覧する通信の暗号化が普及しました。それが「SSL (Secure Sockets Layer) ▶用語集 P.192/ TLS (Transport Layer Security) ▶用語集 P.192」(以下 SSL/TLS) という暗号化通信です。

暗号化していないウェブサイト閲覧では、URL が「http://」から始まるのに対して、SSL/TLS の通信では「https://」で始まります。後ろに追加された s は「secure= 安全な」の意味の s なのです。

## 3.3 https で始まる暗号化通信にはどんなものがあるか

先ほどのチャンネルの話に戻ると、https は通常ポート 443 を使用しま



す。つまりテレビのチャンネルを443にあわせたら、放送にはモザイクがかかっていて、有料放送契約者だけがモザイクを解除して見ることができる、というイメージです。

https:// から始まるウェブサイト  
にアクセスすると、通信相手が誰であるかが後ほど説明する電子証明書によって証明され暗号化通信が始まり、アドレスバーに暗号化を示す鍵マーク▶用語集 P.195が表示されるか、問題がないという意味で、前ページ「3.1 無線 LAN の暗号化と VPN の守備範囲」の②や③の表示がなくなります。

この状態になると、「一応は」、ID やパスワードなどを入力しても大丈夫で、「表示される情報も改ざんされていない」ということになります。しかし、なぜ「一応は」かというと、最近ではこの状態でも安全とは限らないからです。

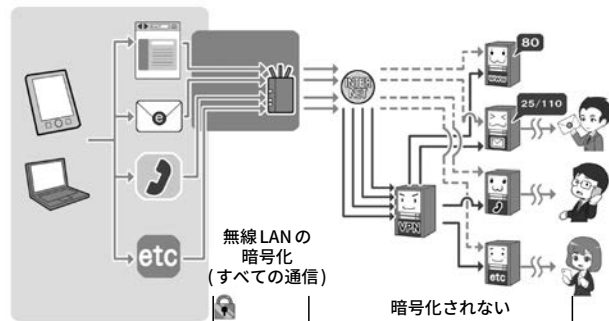
https による暗号化通信を行うためには、まず、https で通信するサーバを作りたい企業や団体のサイト運営者が、認証局▶用語集 P.200 という機関に、書類で自分の会社の情報とサーバのドメイン名を提示して、ネット上で身元を明らかにするための電子証明書の発行を申請します。

認証局は審査の上、その企業や団体が実在することを確認できれば、「SSL 証明書(SSL サーバ証明書)」▶用語集 P.192 という電子証明書を発行します。

「SSL 証明書」を取得した企業や団体は、https で通信するサーバに「SSL 証明書」を設定し、利用者がアクセスしたときに、その「SSL 証明書」によって、該当のドメインの運営主体と証明することで、互いに安心して暗号化通信が始められるようになります。

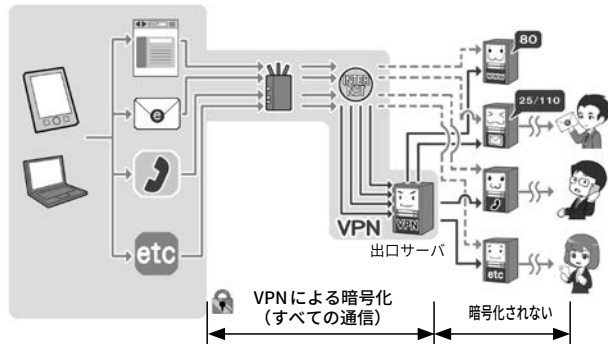
## それぞれの暗号化の守備範囲

### ①無線 LAN の暗号化



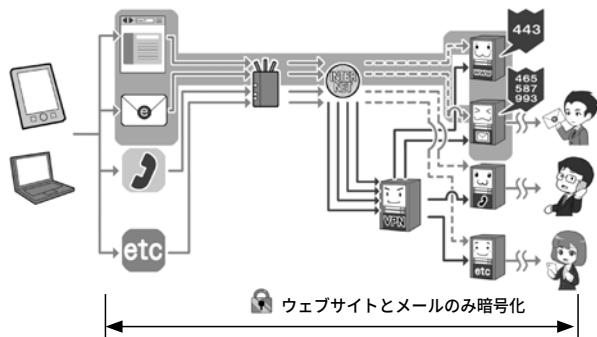
無線 LAN の暗号化は、利用者の機器から無線 LAN アクセスポイントまでのすべての通信を暗号化します。

### ②VPN による暗号化



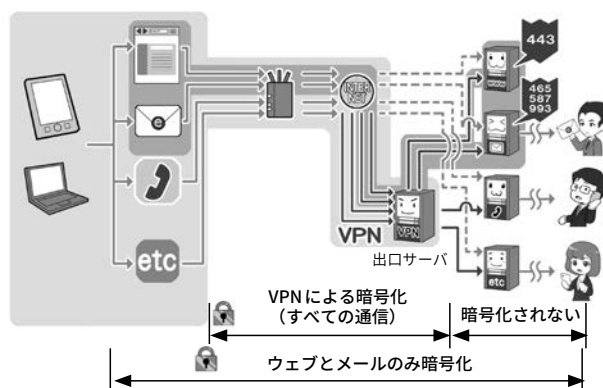
VPN は利用者の機器から、安全とされる「出口サーバ」までの区間で、すべての通信を暗号化します。

### ③ウェブサイトやメールの暗号化



ウェブサイトやメールの暗号化は、利用者のウェブブラウザやメールソフトから目的のサーバまでの区間で、ウェブサイトとメールの通信だけを暗号化します。

### ④VPN + ウェブメールの暗号化



ウェブサイトやメールの暗号化と VPN を組み合わせて利用することももちろん可能です。この場合暗号化される通信範囲は広がります。

しかし、SSL証明書の中には実在性確認をせず、簡単なオンラインでの確認だけで機械的に発行し、企業や団体名すら証明書に記載しないものもあります。そのような「SSL証明書」は誰でも取得できてしまいます。

攻撃者は、そういった審査の甘い認証局を使って、詐欺サイトのための「SSL証明書」を取得して、暗号化通信をする詐欺サイトを立ち上げます。

そして利用者に、「あ、暗号化しているから大丈夫」と油断させ、パスワードやクレジットカード番号を入力させ盗むという事例が発生するようになったのです。

### 3.4 より厳格な審査の「EV-SSL証明書」

そういった問題に直面して、より審査を厳しくした「EV-SSL証明書」が登場しました。

「EV-SSL証明書」の審査では、証明書を発行する認証局も、外部の監査により基準を満たした者に限定して発行権限が与えられ、証明書を受ける側の企業なども、法的な存在の証明や、管理責任者や役員など複数人への聴取など、従来よりも厳格に審査が行われます。

これにより、「法的・物理的実在性」と「正当性」、結果としての「安全性」などが担保され、詐欺サイトなどの排除が行えるようになったわけです。

この「EV-SSL証明書」に対応したブラウザ▶用語集 P.202では、アドレスバーが緑色になったり、企業名や団体名を表示したり、証明書に会社の所在地が表示されるなど、利用者がより確認しやすい表示が行われるようになりました。

しかし2019年ごろには、主要ブラウザの多くはこのような表示を完全に辞めたようです。

その理由は、「EV-SSL証明書」特有の表示を行っても、利用者の行動に変化はなかったからとされ、平たく言えば、「利用者はそのようなものを確認しなかった」ということでした。

### 3.5 アドレスバー警告表示と、常時SSL化の流れ

また、そもそもウェブ▶用語集 P.194の通信が改ざんされないように「常時SSL化」▶用語集 P.197「暗号化されている状態を標準とすべき」という流れもあり、「利用者が通信をきちんと暗号化しているウェブサイトの運営主体を確認しやすくする」方式から、「通信を暗号化していないウェブサイトを『危険である』と警告する」方法にブラウザを取り巻く動向が変化しました。

そして、本項の冒頭にあったように、暗号化されていないウェブサイトにアクセスしたときは、ブラウザが「安全ではない」と表示したり、警告表示のマークを付けたりするようになったのです。

なお、現在でもパソコンのブラウザなどでは、鍵マークをクリックすると証明書内容が表示されます。

「EV-SSL証明書」を利用しているサイトの場合は、その証明書の詳細まで表示すると、証明書を持っている企業や団体の所在地も表示されるので、そのサイトが自分が見ようとしているサイトかどうか判断する手掛かりになります。スマホの場合は、鍵マークをクリックしても証明書が表示されない場合があるので、残念ながら普遍的に安全性を確認できる方法ではありません。

### 3.6 有効期限が切れた証明書は拒否する

なお、電子証明書には有効期限があり、失効したものは安全ではないと考えるべきです。

有効期限に問題があるなどの理由で、ウェブブラウザやセキュリティソフト▶用語集 P.198が警告を発する場合、そのウェブサイトには接続しないようにしましょう。

きちんとセキュリティに対して必要な手続を行っている会社ならば、証明書の失効前に更新の処理を行い、新しい証明書に差し替えるはずですが、

それを行わない企業は、セキュリティに対して必要な措置をしていないと判断し、したがってそのウェブサイトは安全に利用できないと考えるべきでしょう。

### 3.7 他にも証明書に関する警告が出るウェブサイトは接続しない

証明書が失効している警告以外にも、証明書に関する警告が表示される場合があります。

詳しく分類すると多岐にわたるので、すべては記述しませんが、以下のような例が該当します。

1. 証明書の使い方を間違っている場合
2. 証明書の署名アルゴリズム▶用語集 P.197に問題がある場合
3. 証明書を発行した認証局になんらかの問題がある場合
4. 「オレオレ詐欺」のように認証局でないのに認証局と偽って証明書を発行し、それを使っている場合(通称：オレオレ証明書)▶

用語集 P.195

いずれの場合も、「安全ではない通信」の元凶となります。

証明書の有効期限の問題と同様に、ウェブブラウザやセキュリティソフトが「証明書に関する警告」を発した場合、そのウェブサイトとの通信は安全でないと判断し、利用しないようにしましょう。

さて、ウェブサイトを安全に利用するには、通信面の他にも気を付けるべきポイントがあります。

他のセクションとも重複しますが、ウェブを使うというくくりで少し触れておきましょう。

### 3.8 ウェブサービスのログインは多要素認証を選択する

ウェブサービスを安全に利用するには通信の暗号化も大切ですが、ウェブサービスにログインするIDやパスワードの管理と運用も大切です。

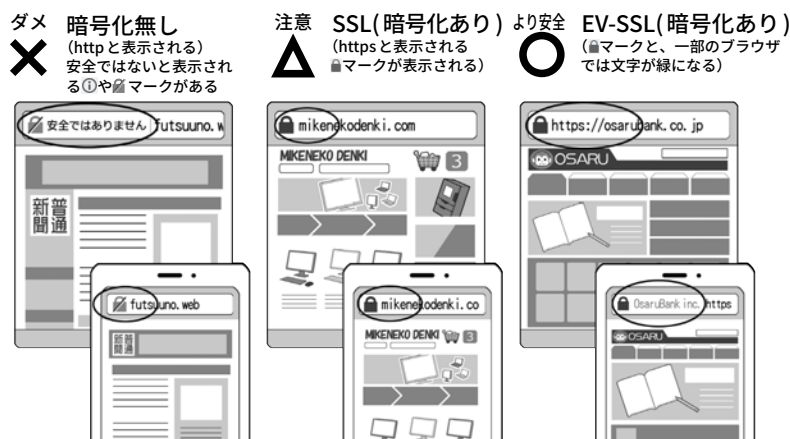
通信を暗号化しても、スマホやパソコンがマルウェアに感染してしまえば、通信する前の段階で情報が盗まれてしまいますし、ウェブサービスのIDやパスワードが盗まれると、攻撃者がウェブサービスに勝手にログインして、悪さをする事ができるからです。

これを避けるため、P.118でも触れたように、ウェブサービスへのログインは、使い捨てパスワード(ワンタイムパスワード)を含む、二要素以上の多要素認証を利用して、仮にパスワードが盗まれた場合でも攻撃者が簡単にログインできないようにしましょう。不審なログインがあった時にログイン通知を受けとれる機能があれば利用して、攻撃を即座に察知できるようにしましょう。

また、近年、ウェブサービスへのログインに関して、そもそも「ネッ

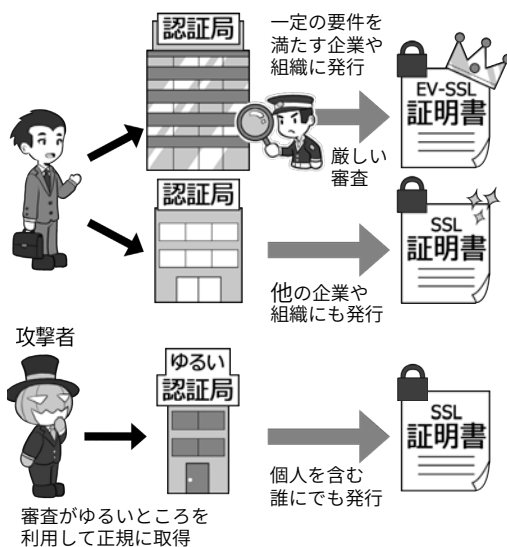
## httpsの暗号化通信で情報を守る

### 個人情報の入力には基本的には……



個人情報の入力をする場合、暗号化は必須となります。厳しい認証局の審査を伴うEV-SSLのウェブサイトを利用する方が、より安全であると判断しましょう。とくに、お金関連のサイトはEV-SSLの方がより推奨されます。

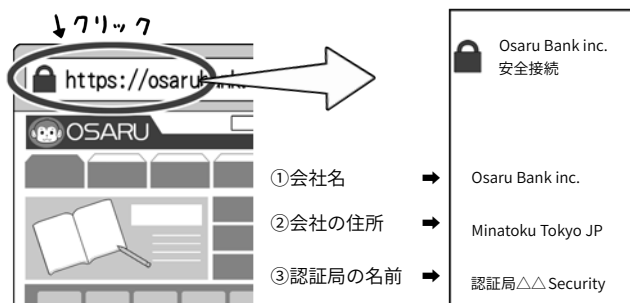
## 攻撃者が不正に取得した証明書に注意



SSL証明書には、ウェブサイトを運営する企業や組織が実在することを認証局が審査して証明してくれるものと、その機能がないものがあります。SSL証明書は元々、サーバ設置者の身元証明のためのものですが、最近では実在証明がなくても証明書を取得できる手があるので、攻撃者が攻撃サイト用に取得することもあります。

EV-SSLのhttpsサイトは、より厳密なので不正取得は困難ですが、上記のとおりただのhttpsサイトは運営者が不明な場合もあるので、要注意です。

## 証明書の内容をチェックする



パソコンなどの場合は簡単に証明書の内容をチェックすることができます。会社名や認証局の名前、EV-SSLに対応したウェブブラウザならば会社の大まかな住所も表示されます。また、一部ブラウザである緑文字のURL表示はEV-SSL証明書の証でもあるので覚えておきましょう。



トを通じて認証のためにパスワードを送信する」という構造そのものが危険だという考え方も出てきています。正当な利用者である認証は、手元の機器の中で行い、パスワードなどは送信せず、「本人であることを確認できた」という認証情報だけをサーバに送って、ウェブサービスを利用可能にする、FIDOなどの方式も一部で採用が始まっています。

今後の動向に注目して、必要に応じて採用するようにしましょう。

### 3.9 多要素認証すら破る「中間者攻撃」

ウェブサービスの安全な利用のためには、二要素以上の多要素認証を利用すべきと本章頭で書きましたが、それすらやぶる攻撃もあります。

例えば、パソコンから二要素認証に対応したインターネットバンキング▶用語集 P.194 を利用する際、銀行のサイトにIDとパスワードでログインするときや送金操作時に、使い捨てのパスワードがスマホに送られて来て、これをパソコンからサイトに入力するとしましょう。

このとき、銀行のサイトだと思っていたものが偽サイトだとしたらどうなるでしょう。攻撃者が、私たちが偽サイトに入力した内容を本物のサイトに中継して、画面の内容をリアルタイムに模倣していたとしても、気付かないまま送金の操作をしてしまうでしょう。

攻撃者が通信を中継しながら、送金先を別の銀行口座に差し替えていたら、二要素認証を使っても不正に送金されてしまいます。

このような、通信経路の途中で双方の通信を中継しながら裏をかく手口は「中間者攻撃」と呼ばれています。

たとえ多要素認証を採用していても、この中間者攻撃をすべて防ぐことはできません。

偽サイトによる攻撃の手法は年々巧妙化しており、ウェブサイトの見た目などから見分けることは極めて難しいのが現実です。そのうえで、注意すべき点を挙げるとすれば以下のことがいえるでしょう。

本物のサイトが、前ページの図にあるようにEV-SSL証明書を使っている場合には、パスワードを入力する直前に、ウェブブラウザ画面のアドレスバーの鍵マークから証明書を表示して、自分の利用している企業や団体名や所在地とあっているか確認する方法もあります。

ただ、先ほど説明した通り、攻撃者が偽のSSL証明書を取得していることを考えると、鍵マークなどの有無だけでは判断できません。

また、アドレスバーのURLを見て自分が知っているウェブサイトとドメイン名が同じかを確認します。

「ドメイン名」とは、例えば「https://www.example.co.jp/foo/bar.html」のうち「example.co.jp」の部分のことです。

ただ、これを確認するのも簡単ではなく、攻撃者は利用者が見間違っているのを狙って、「https://www.example.co.jp.foo/bar.html」という、似たURLで偽サイトをつくることがあります。このURLのドメイン名は「co.jp.foo」であり、「co.jp」とは全く違うところなのですが、「.」と「/」の違いを見抜けないと気が付きにくいのです。

その場合でも、URLの一部をアルファベットに似た別の言語の文字を使って(例：アルファベットの「o」とキリル文字の「o」など)URLを偽装する手口もあります。

こういった状況を総合的に鑑みると、自分が利用するウェブサービスは、基本的にあらかじめブックマークしておいて、訪れる際も、詐欺に用いられやすい偽サイトへの誘導に使われるメールやメッセージのリンクは利用せず、直接ブックマークを開いてクリックして訪れるか、スマホの場合は公式のアプリを利用するのが安全でしょう。

もう1つ注意したいのは、野良Wi-Fi▶用語集 P.200 や、公衆無線LANを利用する時に同名のSSIDに偽装した攻撃者のアクセスポイントに誤って接続してしまうケースです。

安全でないアクセスポイント(P.94の図で接続が×や○になっているもの)に接続している場合には、DNSハイジャックといって、通信経路を誘導する情報が改ざんされ、ブックマークから正規のサイトへ接続しようとして、ブラウザ上も正規のサイトに接続しているように見えても、実際は偽サイトに誘導されてしまう場合があります。

野良Wi-Fiや運営主体の分からない公衆無線LAN、同名のSSIDのアクセスポイントがある場合の利用は避けるようにしましょう。

### 3.10 ウェブサイトを使ったサイバー攻撃に対応する

スマホやパソコンがマルウェアに感染したことによる、パスワードなどの情報流出。事態が起こるまでには、マルウェアに感染する経路が必ずあり、それがウェブブラウザであることもよくあるケースです。最近では、ウェブブラウザでウェブサイトを「見る」だけで感染させる攻撃も発生しています。

攻撃者があなたに、マルウェアを



仕込んだウェブサイトのURLをメールやアプリのメッセージで送り、あなたがリンクをクリックして悪意のあるウェブサイトを見てしまう場合（フィッシングメール▶用語集P.201）や、あなたの行動パターンを調べて、よくアクセスするウェブサイトに、事前にマルウェアを仕込んでおく水飲み場攻撃▶用語集P.203、さらにわざわざお金を払ってマルウェアが含まれた動画広告などを目的のウェブサイトに出すという方法（マルバタイジング▶用語集P.203）もあります。

また攻撃は不特定多数を対象に行われる場合もあります。とくに、広告を使うものは、攻撃者は広告費以上のお金を稼がなければならず、攻撃は無差別に不特定多数に対して行われ、母数を多くとる分被害者も大変多くなります。

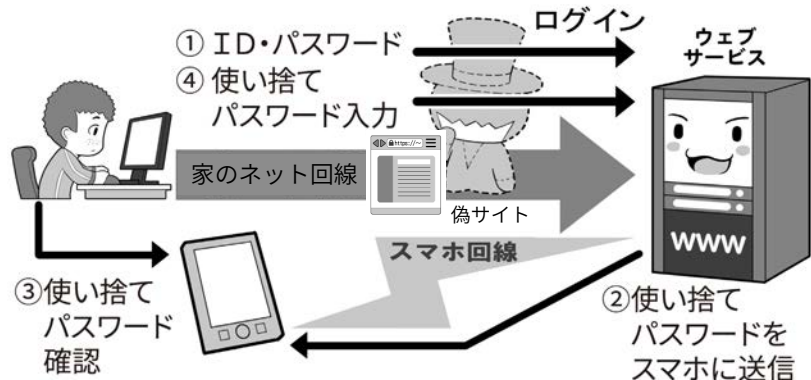
この「見る」だけで感染するサイバー攻撃は、未知のセキュリティホール▶用語集P.198が突然狙われる場合もあるのですが、ネットでセキュリティホールが公表され、メーカーがそのソフトやアプリを修正するまでの「穴が開いたまま」の期間を狙って攻撃する「ゼロデイ攻撃」▶用語集P.198で行われる場合も多くあります。

また、見るだけでなく、あなたの心の隙を突き、巧妙に誘導して「自らクリックやインストール▶用語集P.194させる」といった攻撃もあり、この場合はセキュリティホールがなくても攻撃ができてしまいます。

なお、セキュリティホールを狙ったサイバー攻撃に対する基本の対策は、システムの状態を最新に保つことですが、セキュリティホールの修正など対応が間に合わない場合は、あなたが意識して攻撃を避ける他対処法はありません。

さらに、利用者を巧妙にだましシ

## 間に入りなりすます中間者攻撃

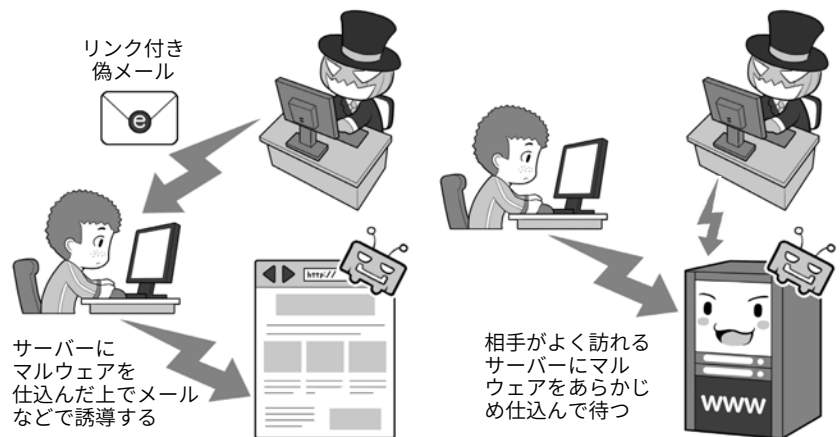


中間者攻撃では、利用者とサーバの間に攻撃者の偽サイトが入ります。攻撃対策として二要素認証を使っている場合でも、改ざんされた情報を見せられたまま処理が進むので、防御が意味をなさないこともあります。

## ウェブサイトを使ったサイバー攻撃の例

### ① 偽メールなどによる誘導

### ② 水飲み場攻撃による感染



システムのセキュリティ設定を変えさせて、自らアプリなどをインストールさせる攻撃に至っては、誰にでもある人間の心の隙の存在を、自分が理解しなければ防げません。

そういった場合に備えて、「不審なメール文中のリンクは開かない」「なにかをインストールさせようとするものは拒否する」「ニュースな

ど情報を常時ウォッチして、特定のウェブサイトやアプリを使った攻撃が判明したらそのサイトやアプリに近づかない」「SNSやウェブサービスの動画や広告は自動再生しないように設定する」などの防御策を積み上げて守りましょう。

## 4

# 安全なメールの利用を支える暗号化について学ぼう

## 4.1 メールにおける暗号化

次は電子メールを安全に使う方法についてです。

「ウェブサイトを安全に利用する」の項目で書いたとおり、メールの送受信もすべての通信の中の一部です。

そして、メールの内容を盗み見されないためには、暗号化の区間が限定される無線LANの暗号化やVPNではなく、メールが送受信中常に暗号化していることが大切です。とくにメールはウェブサイトと異なり、ほとんどが私的な内容になるからです。

メールの送受信では、使用するスマホやパソコンなどのソフトやアプリから、メールサーバまで、送信と受信に別々の通信チャンネルを利用します。

## 4.2 送信の暗号化と受信の暗号化

メールも、昔は送受信どちらも暗号化されていない平文で通信が行われていました。送信を行うSMTP▶用語集 P.192 と呼ばれる通信が25番ポート、受信のうちPOP▶用語集 P.191 と呼ばれる通信が110番ポート、IMAP▶用語集 P.191 と呼ばれる通信が143番ポートを利用していました。

それが、後になって、平文でのメール送信による盗聴の危険性を回避するため、465番ポートを使って、SSL/TLSによる暗号化を組み合わせる SMTP over SSL (SMTPs) が普及しました。これと併せて、メール受信

側の暗号化も普及し、POPがPOP over SSL (POPps : 995 番ポート)、IMAPがIMAP over SSL (IMAPps : 993 番ポート) で提供されるようになりました。

現在では多くのプロバイダメール、携帯電話キャリアメール、フリーメール▶用語集 P.202 サービスで、この暗号化によるメール送受信サービスが基本になっています。

設定が「面倒くさくない」ようにスマホなどでは工夫されていて気付きませんが、最近ではとくに意識しなくても自動的にこの暗号化で通信を行うようになっています。

一方、パソコンのメールソフトでは依然として手動での設定が必要な場合もあるので、パソコンメールを使っている人は一度、自分のメールソフトのメール送受信サーバの設定が、きちんと上記の暗号化ポートや類似の方式を利用しているか、もしくはSSL/TLSなどの文字がある設定になっているかをチェックしてみてください。

とくに、パソコンで古くからメールを利用し、メールソフトの設定を全然変えていない場合、暗号化されていない昔の設定のままになっていることもあります。

メールアカウントをたくさん持っている人は、一度メールアカウントたなおろしの棚卸をし、設定を見て暗号化されていないアカウントがあれば、暗号化している方式に切り替え、暗号化方式がないものしか提供されていないメールサービスは、そもそも安全ではないと考え、暗号化方式が提

供されている安全なメールサービスに乗り換えるようにしましょう。

## 4.3 メールにおける暗号化の守備範囲

先ほども少し触れましたが、メール送受信の暗号化は、スマホやパソコンのソフトやアプリなどから、送受信のメールサーバまでの間を暗号化します。

しかし、目的のウェブサイトの情報を直接閲覧するのとは異なり、メールの送受信は自分が利用しているメールサーバから相手のメールサーバまで、複数の中継メールサーバによってバケツリレーのような受け渡しによる送受信が行われる場合があります。

遠方の誰かに手紙を送ると、複数の郵便局を転送された後に、相手に配達されるのに似ています。

そして残念ながら、このバケツリレー中の送信はいまだ平文で行われていることもあるのです。

自分や相手が契約しているメールサーバまでの経路をそれぞれ暗号化しても、その先のバケツリレーの区間で平文での送信が行われていれば、内容を盗聴されてしまったり、改ざんされてしまったりする可能性があります。

とはいえ、この転送中の通信の暗号化は、大手メールサービス提供会社の努力により進み、改善されつつあります。

ただ、途中の経路をすべて暗号化しても、それぞれのメールサーバで

一旦暗号化が解かれますので、バケツリレーの途中のメールサーバに盗聴しようとする攻撃者がいたら、内容は読まれてしまう余地があります。

それは現代でも外国に郵便を送ると、国や地域によっては検閲で手紙が開封されて中を見られてしまったりとすることがあり得るのに似ています。通信の秘密▶用語集 P.199 が保障されるか否かは国や地域によるからです。

それを避けたい場合は、安全な国内だけで手紙をやりとりするように、メール送受信を暗号化したサービスの中だけでやりとりする方法もあります。

#### 4.4 メール本文の暗号化

ところで、メールの暗号化には、送受信の暗号化ではなく、メールの本文そのものを暗号化する手段もあります。

これには、「S/MIME」▶用語集 P.192 という方法と「PGP」▶用語集 P.191 という方法があります。

これらの方法を使うと、メールのバケツリレーの途中で攻撃者が盗み見しようとしても、もともと本文が暗号化されているため読めません。

メール本文の暗号化には、公開鍵暗号方式▶用語集 P.196 の「公開鍵」と「秘密鍵」を使います。この方法を使うときは、事前の準備として、自分用の秘密鍵と公開鍵を作成しておく必要があります。

相手が自分の「公開鍵」で暗号化したメールを、受信して復号するには自分の「秘密鍵」を使い、相手にメールを送る際は相手の「公開鍵」で暗号化して、送信します。

そしてこれを成立させるためには、お互いの公開鍵を安全かつ確実な方

### メールの送受信は暗号化されているか

メールソフトやアプリが  
暗号通信(SSL/TLS)利用になっているか？

#### メールソフトの例



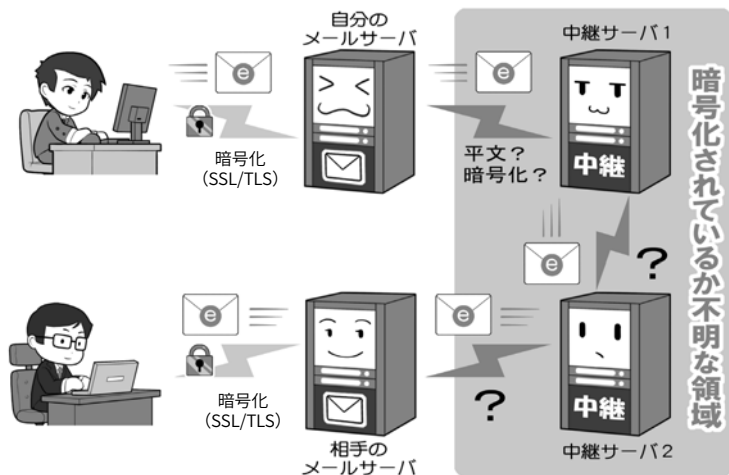
#### メールアプリの例



メールアカウントが設定された状態で、メールソフトやメールアプリの、サーバの詳細設定画面を開き、暗号化を利用する設定になっているかを確認します。

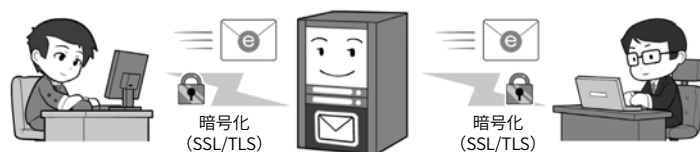
「受信ポート 587 や 993 の使用」「送信ポート 465 の使用」「パラメータ▶用語集 P.201 として SSL 使用がオン」などになっているかがチェックポイントです。これらは暗号化通信が設定されている目印です。

### しかし SSL の通信は自分のサーバまで



メールの暗号化設定は、利用者の機器から契約しているサーバまでの区間のみの暗号化が担保され、メールが送信相手の利用しているサーバに到達するまで経路は担保されておらず、平文で送信される区間がある可能性があります。

### 暗号化している同じサービスを利用する



メールを安全に利用する 1 つの方法としては、暗号化通信を採用した 1 つのメールサービスを、送信相手とともに利用する方法があります。通信の秘密が守られる国内だけで手紙をやりとりするのと同じ概念です。

法で交換しておく必要があります。

とくにS/MIMEを使う場合は、お金を払い認証局が発行する証明書を入手し、自分の公開鍵の正当性を証明する必要があります。事前の準備も必要で、相手も同じことをする必要がありますがあるので負担にもなります。

なお、メールの本文を暗号化しても、メールのヘッダ部分、つまり、件名部分や、宛先と差出人のアドレスなどは、平文で送られることになるので、注意が必要です。

S/MIMEやPGPを使うと、盗聴を防ぐことができるだけでなく、仮にメールの本文を改ざんされても、受信者側で改ざんされていないか調べることができるようになります。また、他人がなりすました偽のメールではないかを確認することもできます。これを実現する技術を「デジタル署名」▶用語集P.199と呼びます。

上記のとおりS/MIMEは大変優れた機能ですが、事前の準備に手間がかかり、大手のメールソフトが対応していないものもあって、残念ながらあまり利用されていません。詳しい方法の説明はここでは省略しますので、各自で調べてみましょう。

なお、利用者ではなくサービス側でメール送信者の成りすましを防ぐ技術として、認証チェックをするSPF、DKIM、そしてこれに引っかけた場合の対処を決めるDMARCなどがあります。これは送信者の書面上のメールアドレスと実際にメールが発信されたサーバのドメインを突き合わせて、合っていないければメールを受け取らないなどの対応ができるものです。

これらを採用したサービスがあれば、積極的に利用を検討してもよいでしょう。それが安全な技術の普及への一助になります。

## 4.5 怪しいメールとはなに か

メールを安全に使うために、メールを使ったサイバー攻撃にも触れておきましょう。

サイバーセキュリティの標語などではよく「怪しいメールを不用意に開かないように」といったものを見ます。

これは「標的型メール攻撃」に代表されるフィッシング(詐欺)メールを使った攻撃に関し注意喚起しています。

この場合、攻撃者が特定の個人を狙って仕事などのメールを装い、マルウェアの添付や、マルウェアを仕込んだウェブサイトのリンクを送り付けるものです。相手が添付ファイルやリンクをうかつに開くと「ゼロデイ攻撃」などを受け、不正なプログラムをインストールされたり、パソコンなどを乗っ取られたりするのです。

実際には、特定の個人を狙った標的型攻撃だけでなく、不特定多数を狙ったばらまき型の「スパムメール」▶用語集P.197でも同様の手口が使われます。誰でも攻撃対象になりうるわけです。

これらの手口は、昨今のセキュリティ環境の向上で「開くだけ」「見るだけ」で感染させることが難しくなったこともあり、少なくとも相手を「感染させるためになにがしかの行動を起こさせる」ことで感染率を上げています。それが偽装したマルウェアをインストールさせたり、偽装広告へのリンクをクリックさせたりする洗練された手法なのです。

こういった攻撃を避け、マルウェアなどに感染しないようにするためには、まず「送られてきたメールの

文面を見るだけで完結しないものは、すべて『怪しいメール』として警戒する」ことが必要です。

送られてきたメールの差出人が知り合いでも、実は全く違う所から送られて来たり、あるいは間違いなく知っている相手から送られてきたメールでも、実は相手のパソコンが乗っ取られていて、そのパソコンから送ってきたりしていることもあります。知り合いからのメールだから安全とはいえないと覚えて下さい。

少なくとも、送られてくることが事前に知らされていない添付ファイルや、「今すぐ確認を!」といったように、緊急に文中のリンクや添付ファイルを開くことを要求するメールなどは、かなり警戒する必要があります。次項目の偽装添付ファイルにも気を付けてください。

発信者に、送信されてきたメールについて「メールではなく電話などの別通信経路」で問合せをしたり、銀行・行政サービス・インターネットプロバイダ・ウェブサービスなどから送られてきた場合は、文中のリンクを開くのではなく、公式のウェブサイトやアプリを直接開き、本当に該当の情報が掲載されているかを確認し、もし個人情報に関わる問題であれば、ウェブサービス側に電話で問い合わせたりするなどの対応をしましょう。

## 4.6 マルウェア入りの添付 ファイルに気を付ける

「怪しいメール」の1つのパターンであるマルウェア入りの添付ファイルとはどういったものなのでしょう。

例を挙げると、業務を装ったメールに「報告書」などの一見文書ファイルなどに見える形で添付されるもの



や、ZIP ファイルというファイルを圧縮した形で添付されてくるものなどがあります。

そして実際は、こういったファイルは本当の文書などではなく、なんらかのマルウェアを含んだ不正なファイルであり、あなたがファイルをクリックして開くと感染するしかけになっています。

通常パソコンではファイルはアイコンで表示され、アイコンには文書ファイルであれば文書ファイルを示す画像が付けられます。

しかし、このファイルのアイコンというものは、簡単に変更可能であり、文書ファイルに見せかけたマルウェアを作ることでも可能で、事実そういった手法が使われます。

ファイル名は、文書ファイルであれば「文書名.doc」、ZIP ファイルであれば「ファイル名.zip」というように、文書の名前の後ろに「拡張子」▶用語集 P.195 といって、そのファイルがこういった種類のファイルであるかを示す文字列が付け加えられます。(表示されていない場合は、ファイル拡張子を表示する設定に変更してください)

マルウェアが実行形式ファイル(プログラム)の場合、拡張子は「.exe」▶用語集 P.190 となり、exe と表示されれば「実行形式ファイルが送られてくるのはおかしい」と気付く人もいます。

これを隠すために攻撃者はファイルの名前を「houkokusyo.doc.....exe」というような長いファイル名にして、後半が省略され画面上で見えないように細工し、文章ファイルに見える「houkokusyo.doc...」の部分だけが表示されるようにして、その上でアイコンを偽装するといったことを行います。

そういった手法に引っかからない

## ウェブメールの送受信は暗号化されているか

鍵マーク



ウェブブラウザでメールを送受信する場合は、ウェブブラウザの暗号化のチェック項目を参考にしてください。

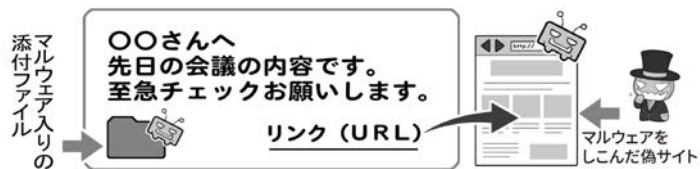
一般的には「SSL 証明書」や「EV-SSL 証明書」を持ち、暗号化通信を示す鍵マークがついていて、暗号化されているかどうか、信頼性があるかどうかなどがわかります。

心配な場合は、パソコンなどでは鍵マークをクリックすることで、そのサーバを運営している主体を確認することができます。

安全性を確認をした上で、「ログインパスワード」などを入力します。

## 怪しいメールとはなにか

### ①仕事のメールを装う



サイバー攻撃に使われる怪しいメールとは、まず「見ただけでは完結しない」メールです。リンクをクリックさせたり、添付ファイルを開かせたり、なにかをインストールさせようとしたりします。

### ②銀行、カード会社、オンラインショッピングサイト、プロバイダ関係を装うメール



また、自分が利用しているウェブサービスの名称で、緊急にどこかのウェブサイトを見させようとするのも、よく使われる手口です。

## 本当の仕事仲間のメールでも攻撃は来る



自分の知り合いや仕事仲間からのメールと思っても安心はできません。名前を語っているだけでなく、攻撃者がその人のパソコンを乗っ取って、知り合いや仕事仲間のメールソフトから攻撃をしかけてくることもあるからです。

ためにも、繰り返しになりますが、「送られてきたメールの文面を見るだけで完結せず、なにか行動させようとするメール」は、すべて「怪しいメール」として警戒することを心がけてください。

こういった攻撃手法は常にブラッシュアップされ進化していくので、定期的に検索エンジンやニュースなどで攻撃の手口を検索をして、最新の攻撃手法の情報を入手してください。

セキュリティソフトメーカーやフィッシング対策協議会、専門機関、識者などの SNS アカウントをフォローすると、最新の情報を入手しやすくなります。

#### 4.7 ウェブサービスなどからのメールアドレスの流出

「標的型メール」▶用語集 P.201 や「スパムメール」による攻撃には、送り先となるメールアドレスが必要です。

メールアドレスを無差別に生成し送り付ける方法もありますが、ウェブサービスなどから流出した大量のメールアドレスを使って送られる場合も多くあります。

会社内で標的型メールによって感染した端末があると、そこから社内のメールアドレスが流出して、さらなる標的となる場合もあります。

こういった情報は、攻撃者によって直接、攻撃メールの送付先として使われるだけではなく、インターネットの闇サイト(ダークウェブ)で名簿として売買されることもあります。

攻撃のメールが送られてきたらもちろん警戒すべきですが、それ以前にもできることがあります。

セキュリティ識者のトロイ・ハインド氏が運営する、「Have I been pwned」というウェブサイトなどで

は、メールアドレスやパスワードなどの流出情報を、すべてではないものの検索できるようになっており、そこで自分の情報が流出した形跡がないかを、ある程度チェックできるのです。

では流出が判明した場合、速やかに対処するのは当然として、流出に備えてメールアドレスにどのような工夫ができるのでしょうか。

#### 4.8 流出・スパム対策としての、変更可能メールアドレスの利用

解決策としては、親しい人とやりとりをする大事なメールアドレスと、ウェブサービスや通信販売サイトなどに登録するメールアドレスを別にし、後者にはメールアドレスを気軽に変更・追加・削除したり、複数の仮想メールアドレスを作れるものを使う方法があります。

これは「メールのサブアドレス」や「使い捨てメールアドレス」▶用語集 P.199 「捨てアド」と呼ばれるもので、ウェブサービスなどからメールアドレスが流出してしまっても、すぐに変更するかメールアドレスごと削除して、攻撃メールが送られてくるのを避けることができます。

思い入れがあり変えられないアドレスと違い、ウェブサービスなどに登録するアドレスは、すっぱりと変えたり捨てたりできるものを使いましょう。

1つのサービスからの流出によって他のサービスに登録しているメールアドレスを変更するのが面倒ならば、無限に近いサブアドレスを作れるサービスもあるので、それを利用してサービス毎に別々のアドレスを登録しましょう。

余談ですがこの方式であれば、攻

撃者からスパムメールなどが来たときに、どのサービスから流出したかを知ることもできます(右下図参照)。

なお、親しい人に限定して使っているアドレスでも、相手がマルウェアに感染して流出させる可能性もあります。さすがにその場合までは対処することができません。

ただ、逆に自分が流出させて迷惑をかけてしまう可能性もあるので、セキュリティを固め、まずは自分から流出させないようにしましょう。

#### 4.9 通信の安全と永続性を考えた SNS やメールの利用

メールの送受信での秘密を確保する手段として、送信者と受信者が「メールの送受信を暗号化している同じサービスを使う」方法について触れましたが、この「閉鎖された空間による安全性の確保」は、「すべての通信の暗号化を宣言している SNS サービスを使ったメッセージのやりとり」にもあてはまります。

この場合、上記のメールサービスの利用と同じく、サービス全体が1つのセキュリティ方針で守られるので、安全性は確保されます。

ただし、SNS の運営企業によっては、すべての通信を暗号化しているかどうかを明確にしていない場合もあり、一般の利用者が自力で暗号化の状況を調べるのは容易ではありません。

現状では、検索エンジンで「自分が利用している SNS の名前」+「暗号化」などと入力して調べるか、暗号化を明言している SNS サービスを選ぶしか方法がありません。本来であれば全 SNS サービスが、暗号化とセキュリティの向上に対応してほしいところです。

この閉じた空間による安全性の確保は、確かに安全な通信に有効な手段である一方、さまざまなシステムや機器がつながりあって情報をやりとりする、「インターネット」の思想とは逆の発想でもあります。

本来は多様なサーバがつながりあってバケツリレーが行われるメールであっても、すべての過程で暗号化が行われ、安全性が確保されることが理想なのです。

一方、現状では問題が残るメールですが、SNSと比較したメリットもあります。

メールは特定の企業サービスとは紐付かないインターネットの仕様なので、さまざまなメールソフトを使い、どのメールサーバに接続しても基本的には利用可能なのです。

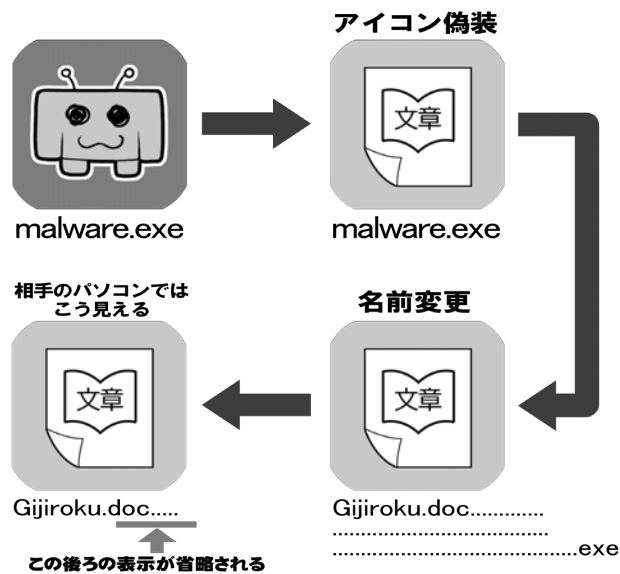
1社によって提供され、栄枯盛衰によってサービス終了する可能性があるSNSに対して、メールは永続性の点で有利といえます。

事実、インターネットの初期からさまざまなOS▶用語集 P.191やメールソフトを乗り継いでも、きちんとメールの内容を引き継ぎ、ごく初期のメールをきちんと見られる状況にしている人が少なからずいます。

SNSや各種通信サービスなどはサービス終了時にデータのエクスポート(出力)の対応をしますが、それらは保存されるデータであって、データが生きていた環境はサービス終了とともに終わってしまうわけです。その分、メールにはない、さまざまな華やかな機能を楽しむこともできます。

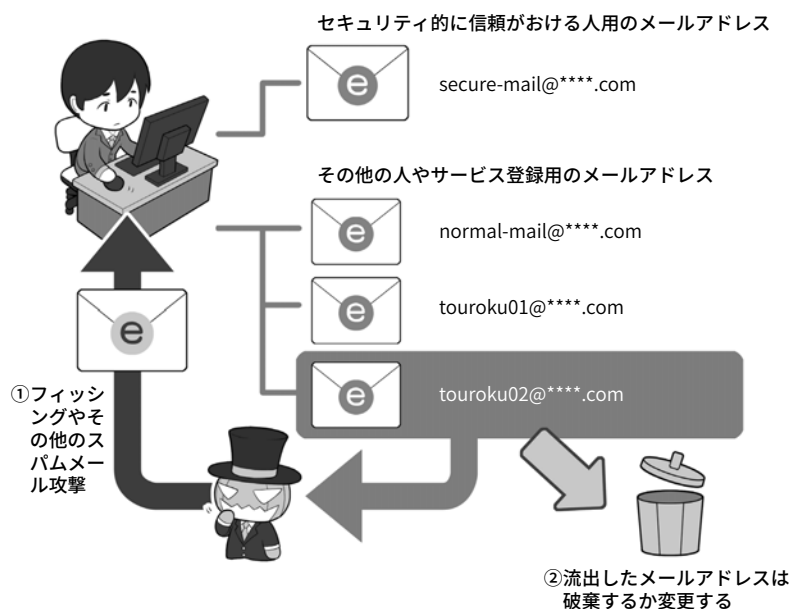
SNSとメール、どちらがよいかは人それぞれです。それぞれにメリットとデメリットがあるのでよく機能を理解して、自分に合ったものをうまく利用しましょう。

## マルウェア入りファイルの偽装



攻撃メールに添付されてくるファイルは、一見するとただの文章ファイルに見える場合もあります。しかし、ファイルのアイコンも名前も偽装したり、別のものに見せかけることは可能なのです

## メールアドレスを変えてスパムメールから逃げる



メールアドレスの流出は、ウェブサービス側で管理しているものが攻撃者によって盗まれたり、ウェブサービス側の内部の人間が持ち出して売却したり、セキュリティ意識のない人がマルウェア感染して流出させることなどで起こります。

愛着を持って長く使いたいメールアドレスは、むやみに人に教えたりウェブサービスに登録したりしないようにしましょう。

流出してしまった場合に備えて、変更したり捨ててしまえるメールアドレスを活用しましょう。

# 安全なデータファイルの利用を支える暗号化について学ぼう

もう1つ、通信にまつわる安全で考えなければならないのは「ファイルの暗号化」です。

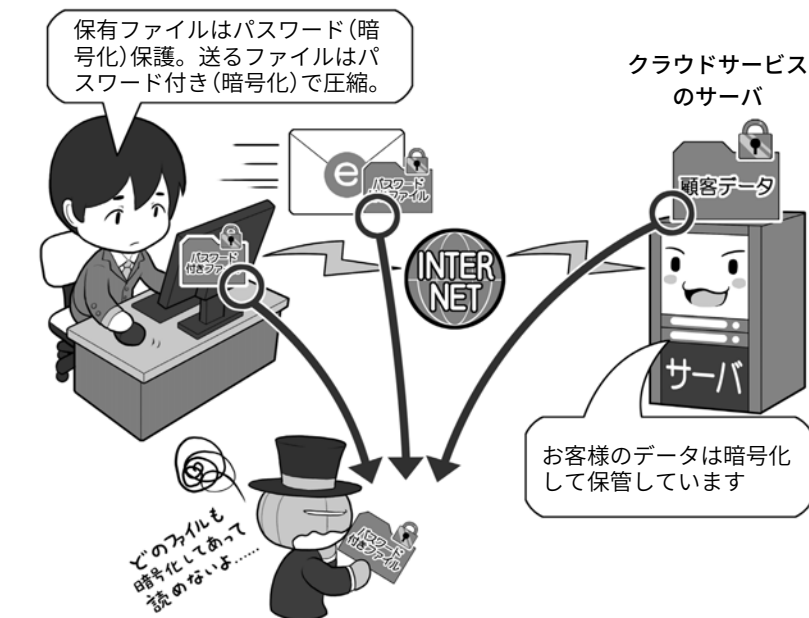
例えば、メールの添付ファイルが盗まれたり、保存しているファイルがマルウェア感染で流出したり、サーバに不正アクセスされて盗み見されても、また、ファイルの入った物理的な記録メディアを紛失しても、確実に適切な方法と鍵(暗号キー)で暗号化してあるならば、攻撃者が解読できなくなり、情報を流出から守ることができます。

ただ、ファイルの暗号化は、攻撃者に盗まれると高速なコンピュータを使って執拗に解読を試みられ続ける可能性があります。したがって「暗号キー」の基準にしたがって、長く複雑なものを設定しなければなりません。

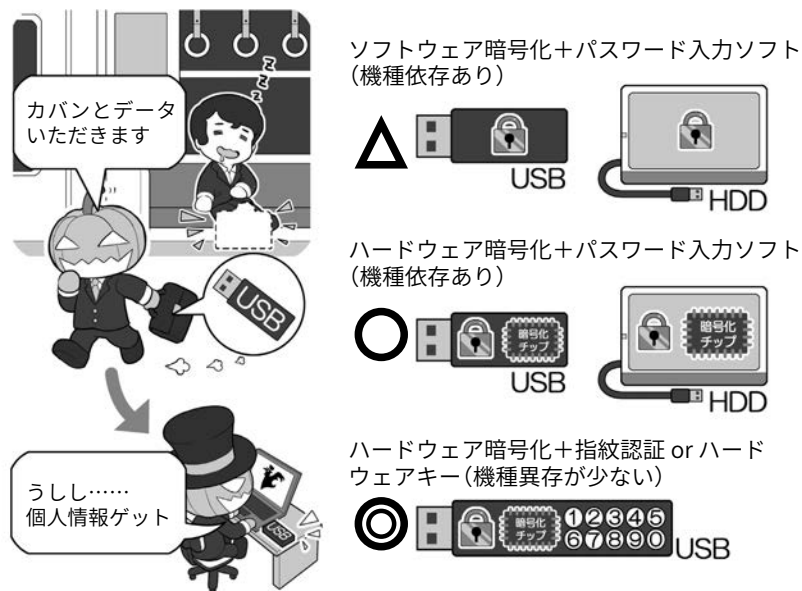
機密情報を持ち運ぶ場合は、ファイル単位の暗号化よりも、装置全体の暗号化機能の付いた外付け記憶装置やUSBメモリの利用を推奨します。2022年6月、兵庫県尼崎市で起きた市民の個人情報記録されたUSBメモリ紛失は記憶に新しいです。このような事態を防ぐためにも、高速に暗号処理が可能でさまざまな攻撃に対策された暗号化チップ▶用語集 P.194 が内蔵された記憶装置を選択しましょう。そうすることで、ファイル単位の暗号化が不確実になった場合のトラブルも避けられます。

USBメモリの場合、汎用性と安全性を両立した、ハードウェアキーでPINコード相当の認証をするタイプもあります。これらは専用の認証

## データの暗号化は保険



## データを持ち運ぶときは必ず暗号化メディア▶用語集 P.194 を使う



+「強制暗号化」+「暗号化方式 AES256bit 以上」  
+「パスワード一定回数入力ミスで完全ロック(アクセス不能)」  
あれば…「書き込み時ウイルスチェック(USBメモリ内機能)」

盗まれたメディアはリモートワイプ▶用語集 P.203 ができないので、より高度なセキュリティが求められます。しかし、それよりも重要情報を持ったまま飲酒したり、電車で寝たりすることは言語道断です。本来は暗号化よりもモラルが第一です。



用ソフトウェアを必要としないので、利用するOSの依存度が少ないのと、ハードウェアキーの入力を「PINコード」方式と同じにすることで、入力を間違えると「ロック」や「データ消去」の保護機能があります。内部では「暗号キー」として十分に長く複雑なものが自動で生成され、この「暗号キー」の利用にのみ「PINコード」の入力を求めることで利便性と安全性を両立しています。

データの暗号化で重要になってくるのは「暗号キー」の運用です。

「暗号キー」は英大文字小文字+数字+記号で、完全にランダムな15桁以上を基準としていますが、完全にランダムな場合、暗記することは困難になりますし、スマホのパスワード管理ソフトやパスワードノートを見て打ち込むのも一苦労になります。

かといって、パソコン上に保存したり付箋で貼っていたりすると「パスワードを利用場所に保管しない」というセオリーに反します。

現状は単純で楽な解決方法はありません。ただ、暗記を前提にするのであれば、自分だけが知っているマイナーな曲の歌詞などからローマ字打ちで15桁よりかなり長くなる部分を抜き出し、独自のルールで一部記号や数字に置き換えて使用などの方法が考えられます。

また、暗号化したファイルを誰かとメールで受け渡しする場合、相手と「暗号キー」を共有する方法にも気を付けなければなりません。

別送信であっても、暗号化ファイルと「暗号キー」を同じメールアドレスに送れば、メールが一気に流出すると2つが揃ってしまいます。

「暗号キー」はメールでは送信せず、現実に入ったときに決めておくか、それができず、出先で突発的に送信

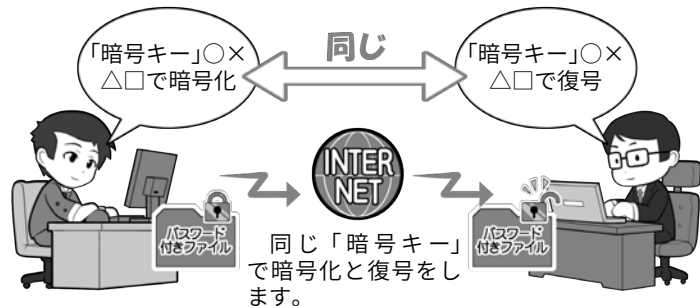
が必要になった場合は、電話などで伝達するか、通信が暗号化されている「別系統の送信経路」で送るようにしましょう。

さらに、「暗号キー」には先ほども少し登場した、対になった2つの暗号キー（公開鍵と秘密鍵）を使ってやりとりする方式（公開鍵暗号方式）があります。この鍵は手で入力するの

ではなくパソコンが自動的に使うためのものですので、こういったシーンでは目にしません。

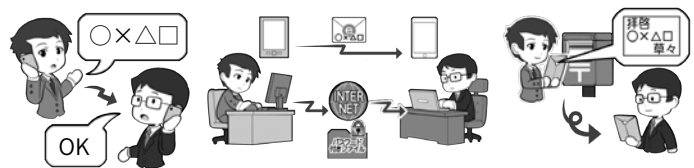
ただ、この方式は、P.139で紹介した「S/MIME」や「PGP」や、同じように目にすることはありませんが、無線LAN通信の暗号化など、見えないところでファイルも暗号化しています。

### 「暗号キー」が1個の方式（共通鍵暗号方式）▶用語集P.195



### 安全な「暗号キー」の受け渡しの例

電話 別経路のメールアドレス 古式ゆかしき手紙



直接会ったときに「暗号キー」を渡したり、電話で直接伝えたりします。

盗聴やマルウェア感染を考え、スマホ対スマホなど別経路で送信します。

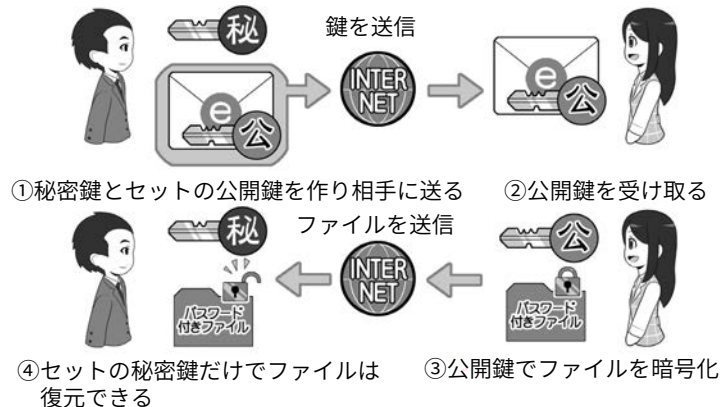
アナログだが1つの方法で、銀行などが利用しています。

どの場合であっても「暗号キー」の秘匿が重要です。

### 「暗号キー」が2個の方式（公開鍵暗号方式）

情報受け取り側

情報送信側



共通鍵暗号方式と異なり、「暗号キー」を送信しても大丈夫なのがポイントです。この方式では「暗号キー」は手入力では使いません。メール送受信の影で使われています。

## コラム.4 「無料」ということの対価はなにか

インターネットではよく「無料」という言葉を見かけます。無料のメールサービス、無料のウェブサービス、無料の動画公開サービス、無料のアプリなどなど。

しかし、お店などの試食コーナーの図を見てもらうとわかりますが、私たち利用者の側から一見無料に見えても、サービスが提供されるときは必ず「コスト(費用)」がかかっています。

そして正常な企業であれば、コストが回収できないビジネスは行いません。そこにはなんらかの採算が取れるシステムが存在し、私たちが見えないところでお金が回って、無料提供されているわけです。

その方法の1つは広告による収益モデルです。広告主がウェブサイトなどに広告バナーを出し、サービス会社はそれを資金源に運営するわけです。

広告システムがもう少し進むと、ウェブサービス会社が私たちのウェブ上での行動パターンや、趣味や行動などの情報を収集し、一見匿名の情報の形にして、これを広告主に提供、広告主は自社製品にマッチした人物向けに絞り込んで広告を打つなどして、より効果的な宣伝を行います。

このパターンでは、匿名とはいえ平たくいえば「私たちの情報」がサービスの対価として支払われているわけです。

また、先行投資といって、当初無料で提供し、利用者がサービスに馴染んだら、その後有料化してコストを回収するマネタイズ▶用語

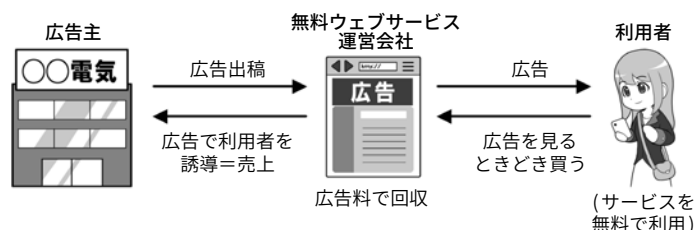
### 試食コーナーのサービスコストの例



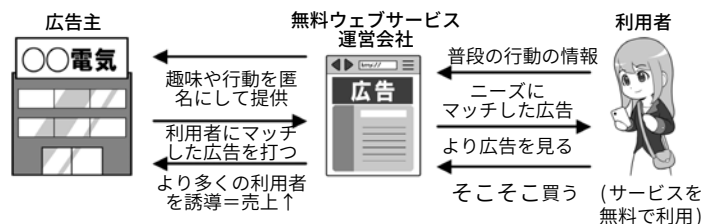
- ・食べる側は一見無料だが、人件費、光熱費、材料費は必ず発生し、どこかで誰かが必ず支払っている
- ・お店全体の売上や直接的なソーセージの売上の一部としてなど
- ・運営主体もしっかりして、コストも回っているので食べても大丈夫

### 無料ウェブサービスの例

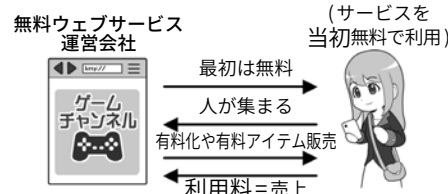
#### ①無差別広告で運営



#### ②利用者の情報を利用し、ターゲットに合わせた広告で運営



#### ③先行投資後マネタイズ(コスト回収)



#### ④セキュリティ意識の低い善意の無料サービス



集P.203 を行う型もあります。

そして最後に最も気を付けたいのが善意の無料サービスです。誰かがウェブサービスやアプリなど

を開発し無料で提供するのは、明示的ではなくても「責任は一切取りませんよ」という状態のものです。

この場合コストは提供する側のポケットマネーなどでまかなわれ、ビジネスとしては成立していないので、セキュリティに対して割くべきコストや労力がおろそかになりがちです。そしてここが弱点として攻撃者に狙われ、利用される可能性があるわけです。

公衆無線LANの無料サービスも考えてみましょう。

政府機関・施設や自治体などが提供するものは、運営費とセキュリティの費用が、実は税金でまかなわれています。

携帯電話会社が提供する場合は、支払料金の中からまかなわれているので「追加料金無料」といった方がよいでしょう。

対価を払って利用する場合は、当然その支払料金が運営管理費用やセキュリティ費用にあてられます。

そして今回も問題なのは「善意の無料サービス(ただし責任能力なし)」です。

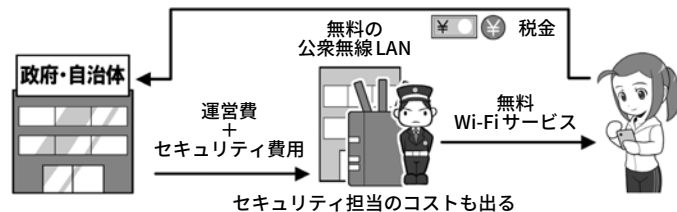
小さなお店などで無線LANが提供されている場合、それは自宅用や仕事用のものを無料開放しているだけかもしれません。そして無料で使っている以上利用者とは契約関係もなく、利用する側は安全性を求める権利もないわけです。

そして攻撃者はこのような所を狙って罠をしかけてきます。運営費もセキュリティ費用もないならば、誰も日常的に攻撃者が忍び込み罠を張っているかどうかなどチェックしないからです。

このような理由があるので、「運営主体がはっきりしていない、セ

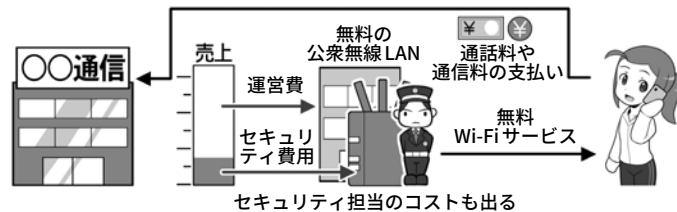
## 無料の公衆無線LANサービスの例

### ①一見無料だが税金などでまかなっている間接的に有料



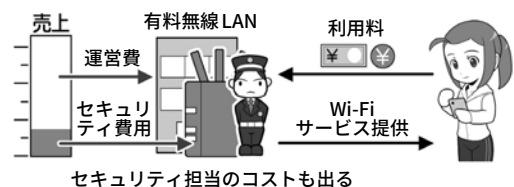
トラブルがあると議会などで取りあげられ問題となることもあります。責任能力もあります。

### ②企業が収入の中から払っているから(追加料金)無料



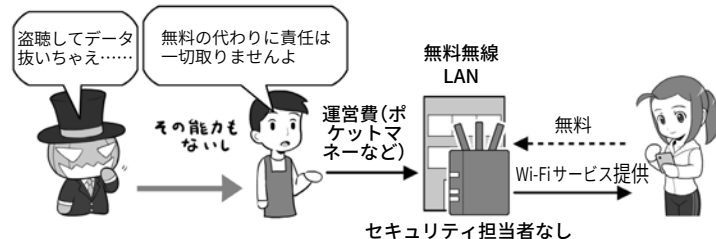
トラブルが起されば責任問題となり、本業にも影響が出ます。責任能力もあります。

### ③対価を支払って利用する(有料)



対価をもらったサービスなので、トラブルが起されば責任問題となります。

### ④セキュリティ意識の低い善意の無料サービス



対価はもらっていないので、トラブルは自己責任といわれたり、実質的に責任は取ってもらえません(その能力もありません)。

セキュリティ意識の低い、無料の公衆無線LANは推奨されないというわけです。

無料という言葉には注意が必

要です。運営されてる費用の出所がはっきりしない場合、あなたが個人として高いツケを払わされることになるかもしれませんよ。



## コラム.5 クラウドストレージサービスからの情報流出。原因は？

クラウドストレージサービスとは、「従来手元で保存していたデータなどを、インターネット上に存在しているサーバに保存し、ネットにつながったどの機器からでも利用できる」サービスです。ネットワークの図の上にインターネットを描く場合、雲(英語でクラウド)を描くことが一般的であったことから、インターネット上で提供されるサービスをクラウドサービス(略してクラウド)と呼ぶようになりました。

とくに、スマホとクラウドは切っても切り離せないものとなっています。スマホを利用していると、意識しないうちに写真などがクラウドサーバ▶用語集 P.195 にバックアップされていることもあります。スマホからでもウェブブラウザからでもアクセスできるメールサービスもクラウドサービスです。

パスワード管理アプリ<sup>\*1</sup>の解説では、クラウドを利用することに関して厳しめの論調で解説していますが、クラウドサービスは、どこからでもアクセスできるため、大変便利で、個人でも利用が広がっています。利用においては、セキュリティに気を付けましょう。

まず、クラウドストレージ上に他人に見せたくないデータがあれば、公開設定や共有設定などのアクセス権限に気を付けましょう。誰でもアクセスできる設定になっている場合、自分の知らないうちにデータを他人に見られてしまうかもしれません。

また、他人にIDとパスワードを知られてしまうと、自分になり

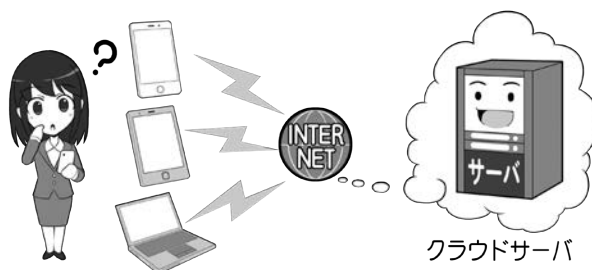
すまして不正アクセスされてしまいます。有名人が狙われるケースや個人がストーカーなどに狙われるケースの原因の多くは不正アクセスであり、不正アクセスを狙う攻撃では、パスワードに対して「リスト型攻撃」「辞書攻撃」<sup>\*2</sup>、そして個人情報からの推測などが行われます。「パスワードは誕生日やニックネームから推測した」という攻撃者の証言もよくあります。

こういった不正アクセスによる情報流出を起こさないためには、まずパスワードを複数のサービスで使い回ししないこと。そして、

推測されるほど簡単なものにしないうこと。セキュリティの強化を目的として多要素認証などや、不正なアクセスがあった場合通知される機能が提供されていれば可能な限り利用すること。そして「本当に流出して困る情報は、クラウドサーバにアップロードしない」ことです。

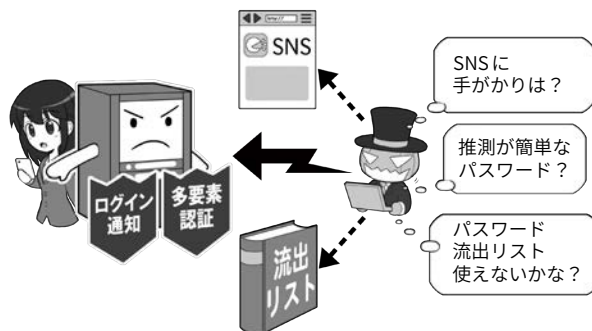
クラウドは大変便利ですが、きちんと利用目的とセキュリティを固めて利用しなければ、攻撃者の格好的になると、理解してから利用しましょう。

### データはどこに保存されている？



スマホなどを使っていると、全く意識せずにクラウドサーバにデータをバックアップしていることもあります。よく分からない場合は、一度調べてみましょう。「クラウド」という名前ではなく、それぞれのサービス毎の名前を付けられている場合もあります。

### パスワードが甘いと流出するかも



攻撃者はクラウドサービスのパスワードを破るために、さまざまな攻撃を試みます。「ログインパスワード」の基準でパスワードを設定するなど、パスワード設定の基本を守るとともに、サービス間で使い回しをせず、多要素認証の設定や不正なログインがあった場合に通知を受け取る設定を活用しましょう。

<sup>\*1</sup> P.33, P.114, P.115 参照 <sup>\*2</sup> P.112 参照



## 第7章

### 中小組織向け

# セキュリティ向上が利潤追求につながることを理解しよう

人材・体制・資金などが限られた中小組織にとって、通常業務をこなしながらセキュリティ対策を講じるための負担は少なくありません。しかし、企業経営においてセキュリティ対策を省くことはできません。セキュリティ対策に投資すべき理由、テレワークを安全快適に利用するために必要なルール作り、企業だからこそ気を付けたいサイバー攻撃、そして最低限把握しておきたいセキュリティ関連の法律などを学びましょう。

#### 1 社内・社外のセキュリティを向上しよう

- 1.1 セキュリティ対策を実施して負のコストを発生させない
- 1.2 セキュリティ対策に必要な投資資金を確保する

#### 2 災害時の会社のために事業継続計画(BCP)を作ろう

- 2.1 打たれ強くあるために、どこでも作業できる能力
- 2.2 人的損失をリカバリする能力

#### 3 テレワークとアウトソーシングをうまく利用しよう

- 3.1 テレワークとBYOD-Bring Your Own Device
- 3.2 効率的なアウトソーシング

#### 4 ファイルの共有設定や情報の公開範囲を見直そう

#### 5 企業が気を付けたいサイバー攻撃を知り、情報収集に心掛けよう

- 5.1 脅威や攻撃の手口を知ろう
- 5.2 より能動的に情報収集しよう

#### 6 企業が気を付けたい乗っ取りのリスクを理解しよう

- 6.1 サプライチェーン攻撃やオフショア開発によるリスク
- 6.2 問題が起きると事業継続に影響を及ぼす

#### 7 企業が気を付けたいサイバー攻撃の具体例を知ろう

- 7.1 標的型メール攻撃の具体例
- 7.2 フィッシング攻撃の傾向
- 7.3 不正アクセスの傾向
- 7.4 不正送金の傾向
- 7.5 ランサムウェアの傾向
- 7.6 ウェブサービスへの不正ログイン
- 7.7 ウェブサイトの改ざんやSNSの乗っ取り
- 7.8 DDoS 攻撃
- 7.9 サイバーセキュリティ以前の情報モラル教育を怠らない

#### 8 個人情報情報は法律に則り適切に取り扱おう

#### 9 フリー素材の取扱いと著作権について注意しよう

#### 10 取引先の監督を徹底しよう

## 1

社内・社外のセキュリティを  
向上しよう

## 1.1 セキュリティ対策を実施して負のコストを発生させない

業績を圧迫するコストとは、どうやって発生するのでしょうか。1つは業務を遂行する上で支払わなければならないお金が増えるときです。もう1つは、イレギュラーな事態が発生して、そのリカバリ▶用語集 P.203 のために人、お金、時間を割くときです。

この後者のロスというのは、なにか問題が発生してそれに誰かが掛かり切りになり、その期間中「利益を生む」ことができなくなることで発生する完全なる負のコストです。

ただ、トラブルを根本的に防ぐことは難しいので、その発生を予想して備え、利益を生まない負のコストによる業績の下ブレをなくす努力をするわけです。

サイバー攻撃▶用語集 P.196 による突発的なトラブルは、まさしくこの例に当てはまります。したがってサイバーセキュリティを強化して備えるメリットはここにあるのです。

「セキュリティを強化する」といわれても「正直うちが攻撃されるなんて万に1つもないだろう」というのが小さな会社やNPOの運営者の本音ではないでしょうか？

しかし、現在の攻撃者▶用語集 P.196 は、業種や企業規模に関係なく無差別に攻撃してきます。サイバー攻撃の数も被害額も年々増加傾向にあるのです。

近年では「セキュリティ・バイ・デザイン」▶用語集 P.198 という考え方が

## 負のコストの発生例



利益を生むためのコストは必要ですが、備えをしなかったために発生し、そのリカバリのために多大なるマンパワーを割くことは「利益を生まない」完全なる負のコストです。そういつたことが起こらないように準備するコスト（費用）は、実は利益を生むための投資なのです。

## インターネットの利点を生かしてコストを減らす

## オンライン発注



## リモートで打ち合わせ



距離の概念がないので移動にかかる時間が仕事に振り分けられ稼ぐことに回せる！

セキュリティを高めて負のコストを出さない

より安定した事業運営

せっかくのIT投資が、セキュリティの事故が原因で負のコストを生むこともあります。セキュリティもIT投資の一部として捉えることが重要です。

一般的になりつつあります。企業のITシステムや業務プロセスなどを設計する段階でセキュリティ対策を組み込んでおき、サイバー攻撃による

不測の事態に備えるのです。

小さな会社やNPOも例外ではありません。持続的な運営を行うために、きちんと備えましょう。

## 1.2 セキュリティ対策に必要な投資資金を確保する

しかし、「セキュリティに事前に備えるといわれてもそんな資金ないよ…」という経営者の方も少なくないのではないのでしょうか？

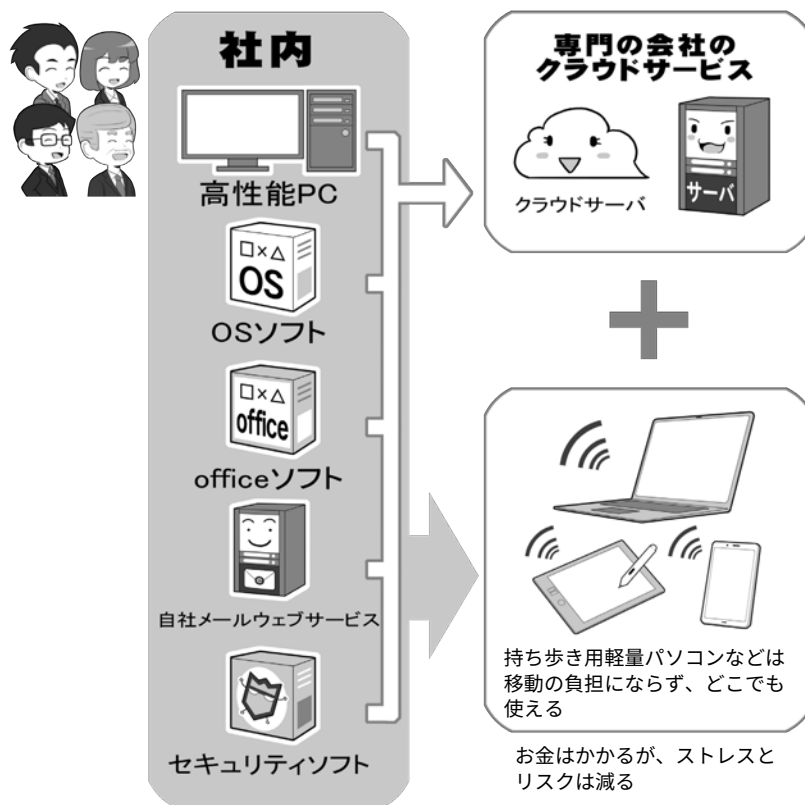
セキュリティ対策が不十分なIT投資は、不必要な「負のコスト」を発生させる可能性があり、予想しない下ブレを起こす原因を抱えていますので、健全な投資とは言えません。また、セキュリティ対策不足によるトラブルは自分たちへの影響だけでなく、顧客や投資家などの関係者にも迷惑をかける可能性もあります。企業や団体の経営姿勢も問われますので、セキュリティ対策を後回しや後付けにせず、セキュリティ対策を含めたIT投資を検討してください。

また、近年では企業の業務システムをクラウド業務スイートに切り替えるケースが増えています。クラウド業務スイートは、業務用ソフト▶用語集 P.198、クラウドストレージ、ウェブサーバ▶用語集 P.194 などが1つのパッケージとして提供され、どこからでもノートパソコンなどでアクセスして業務が行えます。これにより従来は会社に縛られていた従業員がテレワーク▶用語集 P.199 環境で仕事ができるようになったり、スマホを利用して安全に業務連絡を行ったりすることが可能になります。

アウトソース▶用語集 P.193 できることも増えています。自前で対応するよりも外部に委託する方がコストが安く実現できる場合もあります。

こういった新しいシステムや環境は、セキュリティ対策も込みで提供される場合や、これまでバラバラだったコストが集約・整理されて軽くなる場合があり、総コストが従来より

### 面倒なことをアウトソース(外部委託)するのも1つの手



先進的なIT企業では、デスクトップパソコンを廃し、パッケージ版のソフトウェアを廃止し、軽量なノートパソコンと携帯電話回線、そしてクラウドベースのソフトウェアやシステムに活用することで、固定的な机も、オフィスも、出勤すらなくしているケースもあります。また、社内や団体の業務もアウトソースすることで、一層身軽になることもできます。

総務省では「クラウドサービス提供・利用における適切な設定に関するガイドライン」を公開しているので、詳しくは以下をご覧ください。  
[https://www.soumu.go.jp/menu\\_news/s-news/01cyber01\\_02000001\\_00149.html](https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00149.html)

安く済むこともあります。ただし、逆にコストがかかる場合があるので、導入前にしっかり確認しましょう。また、クラウドサービスは設定次第で誰でもアクセスできる場合がありますので、設定に注意して利用する必要があります。

その他、ある程度計画的に時間と費用を取れるのであれば、企業の業務システム構成に、ゼロトラスト▶用語集 P.198 の考え方を採用することで、

テレワーク環境下でより使いやすいシステムにできる可能性があります。

ゼロトラストに即切り替えは難しいことが多いですが、将来を見据えるのであれば検討の価値はあります。

そのようにセキュリティを後回しや後付けにしないIT投資によって業務効率改善が実現すれば、事業運営と高いレベルのセキュリティを両立できます。それが企業や団体にとっての生存戦略の1つになるのです。

# 災害時の会社のために 事業継続計画 (BCP) を作ろう

## 2.1 打たれ強くあるために、どこでも作業できる能力

激しい天災に見舞われる我が国では、災害時にどのように事業継続を行うか、人・モノ・金などの面から事業継続計画 (BCP) ▶用語集 P.190 を、きちんと考えておかねばなりません。その備えがないと、災害時に廃業の憂き目にあう可能性も高くなります。

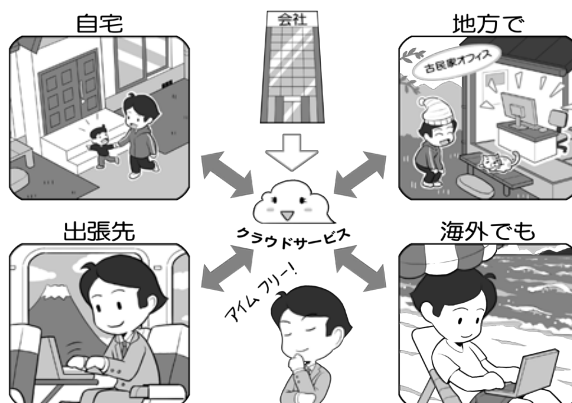
中小企業庁では、「中小企業 BCP 策定運用指針」のウェブサイト\*内で、20 項目による「BCP 取り組み状況チェック」項目を設けています。ここでは IT 関連のアイデアから、その項目を達成するのに役立つと思われるものを紹介します。

最も役に立つのは、ネットがあればどこでも仕事ができるスキルや環境作りです。

生産設備などがあってその場で離れられない職種ではなく、オフィスでの作業を行う業種・職種の人は、インターネットの利点をフルに生かします。データを主としてクラウドサービス上に保存し、あとはアクセスするパソコンなどの機器とネット環境があれば、基本的にはどこからでも作業を行うことができます。

また、作業に利用するソフトを、パッケージ版ではなくクラウド版で購入しておく、災害にあってパソコンが壊れてしまっても、避難先でノートパソコンを購入して、ネットからソフトをダウンロードすれば、かなりのレベルで作業環境を復旧することができます。

### クラウドを活用できれば打たれ強くなる



インターネットとは「距離の概念がない世界」です。これはイコール「どこにでもあるが、どこにでもある」と、少し哲学的な考え方になりますが、うまく使いこなせば、物理的な世界の制約を受けないだけでなく、物理的な世界の災害のダメージを受けにくくなることもあります。

その1つのポイントは、クラウドをうまく使いこなした仕事の仕方だといえます。

最近ではこういったソフトは、クラウド上のデータの閲覧や軽微な修正に関しては、タブレットやスマホからブラウザ▶用語集 P.202 を使って行えるようになっているので、スマホさえ手元があれば、とりあえずは手も足も出ない状況にはならないでしょう。

注意すべき点は3点。1点目はそういったクラウドのデータにアクセスしての作業は、ネットカフェなどでも可能ですが、不特定多数の人が触るパソコンは攻撃者が触っている可能性も高いので、そういった場所での ID▶用語集 P.191 やパスワード▶用語集 P.200 を入力する作業はやってはいけないこと。

2点目。災害時には被災者が通信を円滑に行えるよう暗号化▶用語集 P.194 されていない無線 LAN▶用語集 P.203 が各所で提供されます。これも攻撃されやすいポイントなので、使用する場合は VPN▶用語集 P.193 を使うこと。

3点目として、専門用語では

BYOD (Bring Your Own Device)▶用語集 P.190 というのですが、災害時であっても個人が所有する機器で業務を行っている、うっかりマルウェア▶用語集 P.203 に感染すれば仕事の情報も漏えいする可能性があります。複数台持つのは面倒ですが、セキュリティを鑑み、業務用には別の機器を用意しましょう。

なお、「このどこからでも作業できるというスキル」は、別段災害時のためだけのものではありません。テレワークといって在宅でも作業ができるようにしたり、出産子育て時にも離職しないで仕事を続けられるようにしたり、あるいは地方に出かけて現地のコワーキングスペースを利用することで自由度高く働き、社員や会員のクオリティオブライフを向上させることもできます。

勿論、ためらいなく出張できるフットワークの軽い企業・団体になるには環境作りが重要です。

\* 中小企業庁 中小企業 BCP 策定運用指針ウェブサイト <https://www.chusho.meti.go.jp/bcp/index.html>



## 2.2 人的損失をリカバリする能力

もう1つの備えは、社長や代表者、従業員や会員に人的被害が発生した場合にどう対処するかです。

例えば、社長や代表者が事故で亡くなってしまった場合のことを想定してみましょう。

小規模の企業や団体では専任のIT担当者がおかれておらず、社長や代表者が管理者を兼ねているという例は決して少なくありません。そうした企業や団体では、業務用のIDとパスワードなどの管理をどうするか、事業継続の鍵になる可能性があります。

このため、普段から社長や代表者の他にデジタルデータなどの副管理者を置くなどの手段を取っておくとよいでしょう。いわば人的なバックアップ▶用語集P.201体制です。

そのなかで大切なのは、上記のとおり業務に使われるウェブサービスのIDやパスワードなどの管理です。

もし代表者が管理している場合、そのデータがスマホに保存されていて、その人しか解除するPINコード▶用語集P.191を知らなかったとすると、場合によっては事業継続が困難になります。

先ほども述べましたが、そういった意味では管理用の機器は、個人の機器と分離するということが重要です。そのPINコードなども複数人が持つことが重要です。

また、それが難しい場合は、例えばクラウドでもアクセス可能なパスワード管理アプリ▶用語集P.200を利用し、そのマスターパスワードやPINコードを、弁護士に託し、なんらかの理由で本人による事業継続が困難であると判明した場合は、弁護士に

### 1人しか管理者がいないと…



デジタル化のメリットは、逆に管理者になにかあった場合「物理的な手掛かりがない」ことにもつながります。また、セキュリティをきっちり固めることは、その入口の鍵をなくすとすべてにアクセス出来なくなる可能性もあります。したがって、トラブルが起こったらどうやってリカバリするか、あるいはデータのバックアップだけでなく、人的なバックアップをどうするかをきちんと考えておかねばなりません。

### 万が一に備えて人のバックアップ

社長代理

データ副管理者

弁護士さん



トラブル発生時の  
手順書を作しましょう



トラブルに対処する手順書は、物理的な災害による建物や機材の棄損、サイバー攻撃の対処などだけでなく、人的な損害に対するリカバリも定めましょう。また、人的なバックアップをすることで、重要なデータへのアクセスする資格を複数の人が持つ場合は、だれがアクセスしたかが明確に分かる仕組みにするか、外部の信頼がおける弁護士さんなどに業務を依頼することなどを検討しましょう。

情報を開示してもらうのです。それは昔、貸金庫の鍵を弁護士にも持っていてもらったのと同じです。

このように災害に遭った場合、どのように事業継続するか、そのバックアップ体制を考えましょう。

具体的に事例をあげ、それにしたがってどのように解決するか、シナリオを作り、それを社内や団体の中で共有しておくといよいでしょう。すべては「想定外」にならない想像力があるものをいいますから。

# テレワークとアウトソーシングをうまく利用しよう

## 3.1 テレワークとBYOD-Bring Your Own Device

テレワーク、リモートワークという働き方は昔からありましたが、2020年以降のコロナ禍により全国的に普及しました。

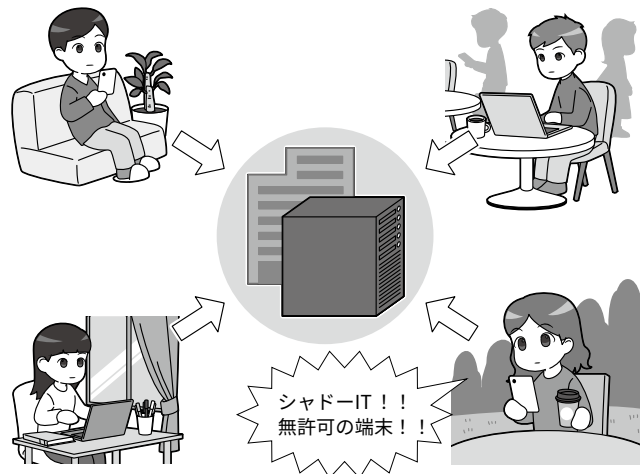
職種や企業などの方針にもよりますが、デスクワークの作業の多くはオフィスに出勤せずとも可能です。現在はクラウドサービスが発達しているので、安定したインターネット環境が整備できれば世界中のどこからでも同じデータを共有しながら業務に従事できます。テレワーク普及によって、BYOD(Bring Your Own Device)という、企業から貸与される端末を使うだけでなく、従業員が個人で所有している端末を業務に使う動きも広がりました。

BYODは、従業員が所有している端末を業務に使うようになるため、従業員が使い慣れた環境で効率的に業務を遂行できたり、企業も端末を配布する費用負担がなくなったりという長所がある反面、端末側に業務情報や認証情報が残ったり、企業が貸与する端末と比較してセキュリティレベルが劣ったりする短所、懸念もあります。

BYODの実施にあたっては、従業員が端末を盗難された場合など、想定されるセキュリティ上のリスクを企業側が事前に把握しておく必要があります。

BYODの実施には企業が運用のルールを設定すべきですが、このルールを理解しない一部の従業員が「シャ

### BYODと気を付けたいシャドーIT



シャドーITはBYODを実施する企業でよく起こる問題です。企業側は、従業員が端末を盗難された場合など、想定されるセキュリティ上のリスクを企業側が事前に把握して、従業員が効率的に業務を遂行できる環境を整備しましょう。

#### テレワークにおけるセキュリティ確保 | 総務省

[https://www.soumu.go.jp/main\\_sosiki/cybersecurity/telework/](https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/)

#### テレワークセキュリティガイドライン(第5版)(令和3年5月) | 総務省

[https://www.soumu.go.jp/main\\_content/000752925.pdf](https://www.soumu.go.jp/main_content/000752925.pdf)

#### 中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト) | 総務省

[https://www.soumu.go.jp/main\\_content/000816096.pdf](https://www.soumu.go.jp/main_content/000816096.pdf)

ドーIT」という問題を起こすことがあります。シャドーITとは、企業が許可していない端末やサービスのことを指し、従業員が許可していない端末から社内のシステムを利用してしまうケースがたびたび生じるようです。例えば、業務連絡にLINEなどを使用していたら、従業員の転職後、知らずとも自社の秘密情報が他社に知られてしまった、といったリスクもあり得ます。

しかし、シャドーITは従業員が社内の環境や端末に不満を感じているからこそ生じがちな問題であり、従業員がシャドーITを使わなくても効率的に業務が遂行できるよう、企業側で社内の制度や設備を整備する、というアプローチも考慮しましょう。

総務省もテレワークの環境を整備しやすくするため、ガイドラインや手引きを公開しているので、積極的にチェックしてください。

## 3.2 効率的なアウトソーシング

もう1つのインターネット時代のメリットは、気軽に専門的な業務をアウトソーシング(外部委託)できることです。

従来であれば、なにかモノを発注する、業務を委託するといった場合、物理的な距離に縛られました。しかし、現在では、自分が望むサービスをインターネット上で検索すると、さまざまな専門の業者を、オンラインで見つけることができます。

例えば、例えばチラシやパンフレット、および印刷物全般などは、オンラインの印刷業者がウェブサイトを設けており、そこで目的のものを探して紙質などを指定すると、どれぐらいの部数がどれぐらいの印刷日数で、いくらぐらいでできるかが明確になっています。

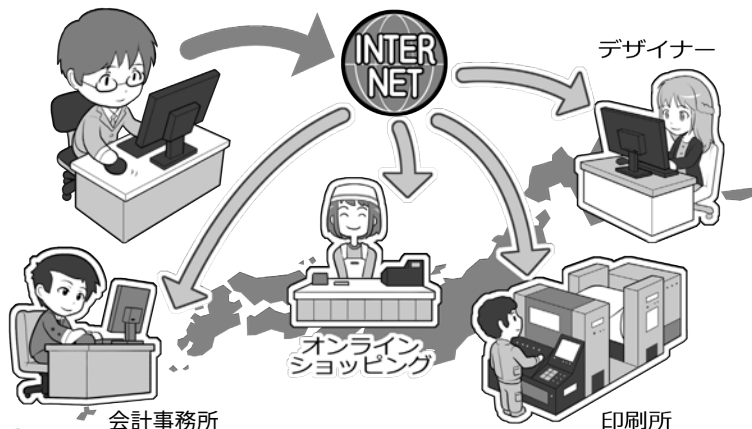
あとは発注側が、業者が受け付ける形式のデータを作るスキルがあれば、24時間365日印刷物が発注できるわけです。

また、経理処理なども会計ソフト会社がオンライン対応になることで、取っておいたレシートをスキャナやスマホの撮影機能経由で提供されているクラウドサービスにダイレクトにアップロードすると、基本的な伝票入力が行われた状態で会計ソフトに返ってくるようになっているものもあります。

仕事で使う資材でも、図面を送信すれば、金属板をレーザーでカットして穴開けまでしてくれたり、簡単な折り曲げ加工をしてくれるもの、あるいは従来ならば専門店でしか購入できなかったものが、オンラインで購入できたりします。

そうすることで、いままでの業務

### どこにいても仕事ができる



社員がどこにいても仕事ができるのと同様に、地方に住んでいる専門分野の人たちと仕事をする制約も少なくなります。場所ではなく求める技術を基準にフリーランスの人を探して仕事を依頼することもできますし、自社で原稿だけを作り、制作や印刷といった後工程の業務を、遠方のプロにオンラインで発注することもできます。場合によっては特定の業務を行う自分の手間と発注のコストを計算して比較して、それをアウトソーシングすることで、自社や自団体が自らが得意とする分野に注力して能力を向上し、逆に選んでもらえるプロになりましょう。

### セキュリティ系業務もアウトソースできる

日常的なサイバーセキュリティに関する業務も、専門業者にアウトソースすることが可能です。どういった企業に依頼したらよいかが判断しにくい場合に備えて、経済産業省とIPAでは一定の基準を設け、これを満たした企業のリストを公開しています。詳しくはP.181を参照してください。

### 製品を扱うなら全世界が市場



自社や自団体が何かの製品や物品をつくって販売や提供する場合も、ネットを活用すればその対象が全世界になるといっても過言ではありません。昔であれば距離の壁に阻まれ小さなマーケットに閉じ込められていた地方都市の小さな会社でも、ネットの時代の特性を活かして、世界的にビジネスを行えるようになった例もあります。

もちろん発信する情報を翻訳したり、時には海外の方とコミュニケーションする必要もありますが、そういった言語的な問題はいずれIT技術で解決されるでしょう。とくに伝統技術などは「存在が知られていない」ことが、海外でのチャンスを逃がしていることもあるのです。

の効率化が行え、必要だったコストや時間を省くことができます。

一方、近年は悪質な業者も増えて

きているため、見つけた業者の評判をインターネット上で探してみることもお忘れなく。

# ファイルの共有設定や情報の公開範囲を見直そう

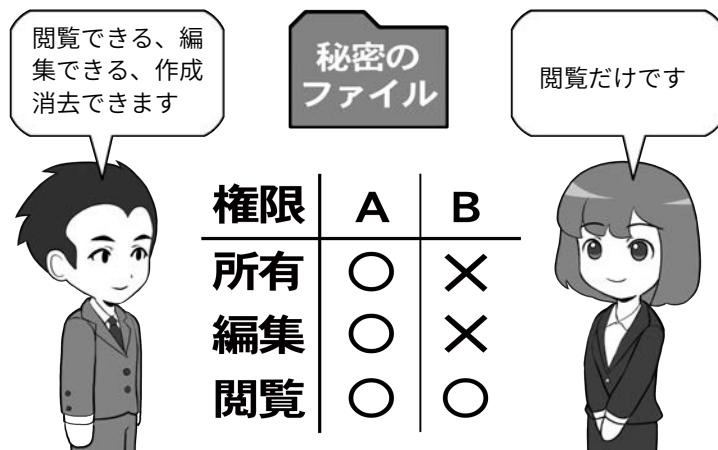
共有設定とは、私たちがIT機器上やインターネット上で使用するファイルや情報、あるいは機器そのものに関して、自分だけでなく誰かと共同で利用するときに、機密性を保つために必要な設定です。

共有設定には、ファイルの管理を例にあげれば、単純に見られるか見られないかを意味する「閲覧」、そのファイルを編集して内容を書き換えることができる「編集」、そしてファイルそのものを作ったり削除したりできる「所有」などの、大まかに3つの権限▶用語集P.196があります。

会社内でファイルをUSB▶用語集P.193メモリのような媒体にコピーしなくても受け渡しをしたりすることを可能にするために、社内にネットワーク(LAN:Local Area Network)を引いている企業であれば、ファイルを管理する「NAS」(NAS: Network Attached Storage)というサーバ上にある文章ファイルなどを見られる人を制限したり、あるいは誰かがうっかりファイルを消してしまわないように、こういったファイル毎の所有者設定や、同様の意味を成す資格設定をしっかりとしておく必要があります。

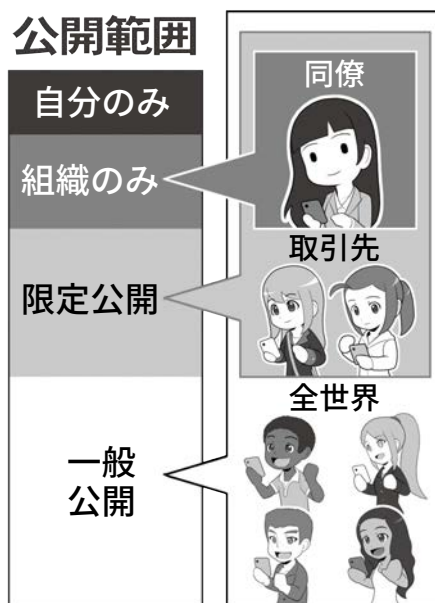
クラウドストレージサービスのようインターネット上のサービスにも共有設定があり、「公開範囲」▶用語集P.196と呼ばれることが多いようです。インターネットのサービスの公開設定を一般公開にした場合、インターネットにアクセスする世界中のすべての人に公開することになりますので、注意が必要です。

## 共有設定ってなんだろう？



物理的な手帳は、それが誰の持ち物で誰にも見せてよいかといったことは、とくに意識せずに使っています。しかし、ネットワーク上にあるファイルなどは、とくに設定しない場合は、「基本的に誰でも見られる」状態になっているので、それでは困る場合、これに対してアクセスを制限する権限を設定する必要があります。それらが「所有」「編集」「閲覧」の権限です。

## クラウドストレージの公開設定



企業がクラウドストレージを用いて自社内や取引先と業務上必要なファイルのやりとりをする際には、公開設定・公開範囲に注意しましょう。自社内に公開を留めておきたい情報を誤って一般公開すると、意図しない人にまで情報が閲覧されてしまう可能性があります。サービスによっては初期設定が一般公開になっている場合があるので、公開範囲は注意しましょう。

この公開設定の初期設定が一般公開になっていたたり、誤って公開範囲を変更してしまったりした場合、情

報が外部から閲覧できる状態になります。何者かに情報を持ち去られたり、公開された情報が原因で報道や



SNSで話題になり炎上▶用語集 P.195 したりした企業の事例もあります。

LAN上のNASでもストレージサービスでも、共有設定はファイル単位やフォルダ単位で設定できるので、その整合性に気を付けないといけないことと、例えば臨時で誰かに特定のファイルを公開したい場合、設定ではなく「見たり編集したりできる」リンク▶用語集 P.204 を送信することで共有することができるものもあり、この場合、そのリンクを知っている人は誰でも同じ権限を持つので、送信後の管理にとくに注意が必要です。

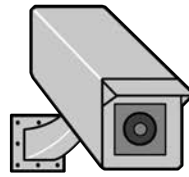
IT機器そのものの利用にも、同様の設定があり、こちらの場合は共有というよりも利用できる権限設定です。機器を管理し設定を変更できる「管理者」や、利用するだけの「利用者」や「ゲスト」などがあり、これらは機器に対してログイン▶用語集 P.204 するときのIDとパスワードで管理されるので、資格管理をしっかりと行って下さい。

権限設定つながりでいえば、会社の建物や特定の部屋に入るための権限を設定している場合も、同じようにきちんとした管理が必要です。例えば人事情報がある場所は人事の人間しか入れないようにしておく必要がありますし、社員の異動や退職が発生した場合、資格の無い人が立ち入りできないように、きちんと設定変更をしたり、入出用にICカードや鍵などを使っている場合は、回収する必要があります。

また、こういったシステムもIT機器を使っている場合は他のシステムと同じように、常にアップデート▶用語集 P.194 する必要があります。それを怠ると攻撃者がシステムをクラッキング▶用語集 P.196 した上で建物に物理的に侵入することもあります。なお、攻

## 機器の共有設定

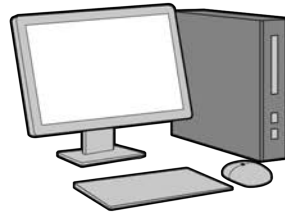
監視カメラ



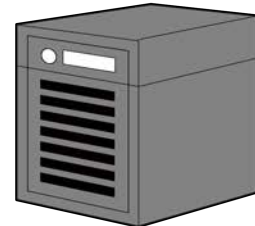
ネットワークプリンタ



パソコン



NAS



無線LAN  
アクセッスルータ  
▶用語集 P.203



スマートロック



社員  
管理者



社員  
その他



退職者



攻撃者



会社や団体の事務所で使用する機器も、ネットワークにつながっている場合、基本的には誰でも利用できる設定になっていることが多いです。したがって特定の人のみが利用できるようにしたい場合は、それぞれの機器および利用者に対して権限を設定する必要があります。

建物などの立ち入りにIT機器による権限を設定している場合は、異動や退職などによってその人物の権限が変更されたり失ったりした際に、それに合わせてきちんと権限を変更するか、権限を執行するためのカードなどを回収しなければなりません。

これを怠ると、退職者が勝手に建物に立ち入ったり、あるいはなんらかの方法で攻撃者がそのカードを入手すると、なんの作業もしないで建物に侵入してしまえます。

また、機器に対する資格設定をしていない場合、攻撃者が無線LAN経由などで建物内のLANに侵入した場合、各種機器やファイルを管理しているNASなどに、なんなくアクセスしてしまえます。複数の人が働く職場ではこういった権限設定はとくに重要です。

撃者は人間の心の隙を突くソーシャルエンジニアリング▶用語集 P.198 で社員をだまし、例えば建物管理や防犯システムの業者のふりをして、堂々

とやってくるかもしれないのでそこらも注意しましょう。人間の心理も攻撃の対象なのです。

# 企業が気を付けたいサイバー攻撃を知り、情報収集に心掛けよう

## 5.1 脅威や攻撃の手口を知ろう

「敵を知り己を知れば百戦危うからず」という孫子の諺<sup>ことわざ</sup>がありますが、サイバーセキュリティ上、危うい状況に陥らないためには、自らのセキュリティ環境が脅威にきちんと対応できてるか知り、また、攻撃者の手口を知ることが重要です。知らないことが、サイバー攻撃による被害がなくなる本質でもあるのです。

それを理解できれば、なにが必要かがわかり、さらにどのような情報が必要か地図が描けます。そうやってサイバー攻撃の危険性(ソーシャルエンジニアリングのような人間の心の隙を突くような攻撃を含め)を知ることが、一番の対策となるのです。

では、どのようにしたら情報を入手できるのでしょうか？まずはセキュリティソフトを提供している企業の発信に注意を払いましょう。そうした企業はSNSなどで最新の攻撃情報をいち早く配信していることが多いので、著名な企業のアカントを複数フォローするとよいでしょう。

次にOS▶用語集P.191を作っているメーカーなどのアカウントです。ただし、そのアカウントが発信するのは自社製品に関する情報のみですが、有益な情報も多くあります。

もっと横断的な情報が欲しい場合は、IPAやNISC▶用語集P.191などの政府機関のアカウントやメールマガジン、セキュリティや詐欺関連の対策機関の公式アカウント、セキュリティ系雑誌の記事を追いかけるようにし

### 攻撃者の攻撃手段を知ること学ぶ



仕事のメールに偽装したマルウェア

セキュリティ企業のブログやセキュリティ系のウェブ記事を見ていると、攻撃者の新しい攻撃手段について、かなり素早く教えてくれます。ニュースをキャッチする他に、それがどういった意味を持つのか知りたい場合は、セキュリティ系ブログや記事が参考になります。

### 公的機関、OS企業、セキュリティ企業の情報を聞く



### 本当にヤバいサイバー攻撃が発生するとこんな感じに



上図に書かれているようにして、広範囲にアンテナを張ると、本当にヤバい攻撃が発生した場合は、各種ソース▶用語集P.198がその性格にかかわらず、一斉に同じ話題について発信し始めます。記事を理解するだけでなく、こういった波を肌で知ると、攻撃の危険度を察知し身構えたり回避策をとったりできます。

ておけば、大規模なサイバー攻撃の兆候やセキュリティホール▶用語集P.198の発覚をいち早く察知することがで

き、その対策を立てることが容易になります。

## 5.2 より能動的に情報収集しよう

そうした必要最低限の情報だけでなく、世界で起きているサイバー攻撃のトレンドなどを知りたいなら、海外のセキュリティ関連企業や機関、サイバーセキュリティに関する情報を提供しているウェブメディア、セキュリティ識者のSNSやブログなど参照するとよいでしょう。

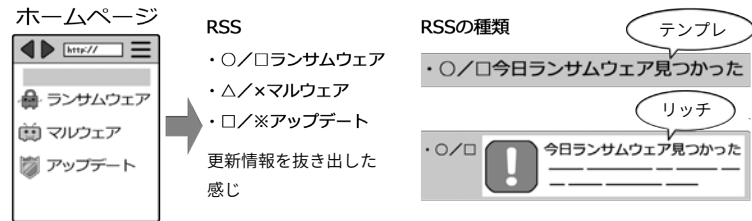
ただし、こうした情報は能動的に収集した上で取捨選択をする必要があります、さらに必ずしも毎日アップデートされるわけではありません。このため初めは熱心に情報を収集していても、だんだんと飽きてきてあまり見に行かなくなるかもしれません。

そこで、RSS ▶用語集 P.192 と呼ばれる仕組みを利用して、攻撃情報を楽に収集できるようにしましょう。RSSは気になるウェブサイトやブログを登録しておけば、記事の更新があれば時系列で情報を串刺しして表示してくれます。

そうしたRSSを簡単に閲覧できるのが、RSSを管理できるウェブサービスとスマホ用のRSSリーダーと呼ばれるアプリの組み合わせです。それらを利用すると、まるでSNSを閲覧する感覚で、毎日世界中のどこかで起きているサイバー攻撃情報やトレンドが読むことができ、否が応でもセキュリティに関しての知識が蓄積されるでしょう。

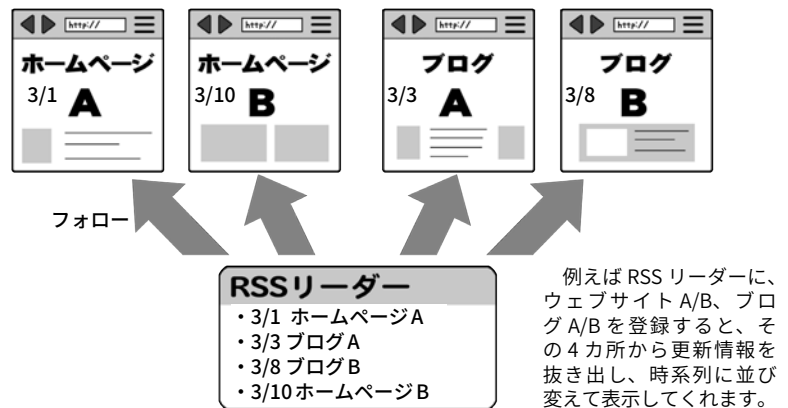
その他、情報を選別するのに長けた企業や専門家が、重要そうな情報を選別・配布するサービスを提供していることがあります。必要に応じてそのようなサービスを受けることも視野に入れて、自身にとって必要十分な情報を取り入れましょう。

### RSSってなんぞや

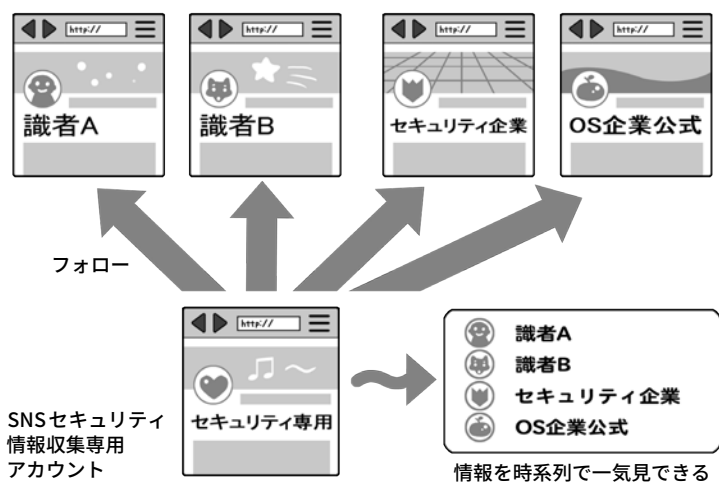


RSSとは平たくいえば、ウェブサイト上の更新情報を見出し、もしくは概略付きで、時系列に、ウェブサイトの裏の見えない所で発信しているものです。規格（フォーマット）が決まっているので、RSSリーダーに登録すると複数の情報源を串刺しして見ることができます。

### RSSは情報を串刺しして一気見できる



### SNSも同様



RSSリーダーの感覚は、SNSで複数のアカウントをフォローすると、素の表示ではフォローしているアカウントの発信が時系列で並ぶのと一緒です。それと同じことをウェブサイトやブログでやると考えると分かりやすいでしょう。

なお、RSSリーダーはインターネット上のサービスで、それ自身がスマホアプリを出している場合もありますし、RSSリーダーに対応した個別のアプリも存在するので、それを導入すると、SNSの流し見と同じ感覚でセキュリティ情報をチェックできます。もちろんSNS上にある、セキュリティ関係のアカウントをフォローしてもOKです。セキュリティ情報収集専用のSNSアカウントを作ってフォローしておくと、個人的なSNS活動と混ざらないでしょう。

よい情報源を集めてこの2つを常時チェックしておくと、かなり情報を素早くキャッチできます。なお、こういったウェブサイトやアカウントで発信される情報は、必ずしも一次情報ソースではないので、真偽を確かめたい場合は一次情報ソースを探すよう心がけて下さい。



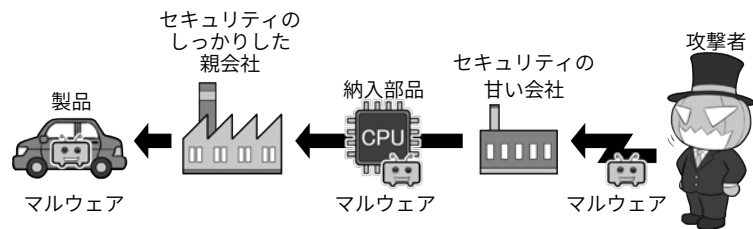
# 企業が気を付けたい 乗っ取りのリスクを理解しよう

## 6.1 サプライチェーン攻撃やオフショア開発によるリスク

「サプライチェーン▶用語集P.197 攻撃」による機器やアカウントの乗っ取りに注意しましょう。「サプライチェーン攻撃」とは攻撃者が、セキュリティが堅牢な大企業を直接狙わず、その企業の業務上や製品調達上の関係があり、かつセキュリティが堅牢でない企業を狙うなどして、攻撃を仕掛ける手法です。業務上つながりがある場合は、乗っ取った企業の従業員のアカウントから、メールをダウンロードして、取引先の相手の氏名やメールアドレスを盗み出し、日常的にやりとりしている文面を模倣して、マルウェア付きのフィッシングメール▶用語集P.201を送り付けます。場合によっては、その人物のアカウントそのものからメールを送る場合もあるため、受け取る側はフィッシングメールを疑う手掛かりがなく、引っかかってしまう可能性が高くなります。

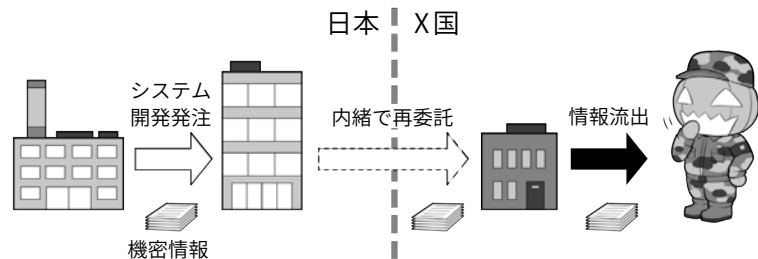
また電子機器を生産している企業などでは、生産しているIT部品にマルウェアやバックドア▶用語集P.201を仕込み、これを大企業に納入させることで、大企業が生産している製品を乗っ取る環境を整えるなどします。例えば大企業へ納入するのがネットワーク部品で、大企業が生産する最終製品がパソコンなら、最悪の場合、マルウェアやバックドアが仕込まれたパソコンが一般流通する事態になります。こういった攻撃に遭うと、サプライチェーンに関係する中小企業や団体にも責任が生じます。

### ① サプライチェーン攻撃とは



サプライチェーン攻撃とは、最終的な攻撃目標を生産している、セキュリティが堅牢な企業を狙うのではなく、そのサプライチェーン（供給の連鎖）の工程の、弱い企業や弱い場所を狙って攻撃を仕掛け、最終的な攻撃目標に、マルウェアなどを仕込む手法を指します。イラストでは車（ハードウェア）が狙われていますが、ソフトウェアであっても同様で、考え方として誰かのアカウントを乗っ取るときにも使われます。

### ② オフショア開発とは



オフショア開発とは、ソフトウェアの開発するときに、受託した企業が依り開発コストが安い海外の企業などに再委託することを指します。しかしこの再委託先が我が国と同じ倫理感や法治の概念を持たず、モラルが低い場合、サプライチェーン攻撃を仕掛けられる場合があります。問題は受託企業が発注企業に内緒で再委託している場合あり、発注者はセキュリティ上、開発がどこで行われるか、契約で定め、掌握する必要があります。

明示的なサプライチェーン攻撃以外にも、気付かぬ所で情報の漏えいを起こすケースにも気を付けましょう。使用するIT機器が、利用者の意に沿わぬ形で情報を勝手に国外に漏えいさせるケースもあります。

通信機器やドローンに関連したサイバー攻撃が取り沙汰されている他、外部から不正にIT機器へのアクセスが可能となるバックドアの設置も話題になっています。機器を購入するときは、当該の会社の製品が、類似のトラブルを起こしていないか、

入念に調べてから手配しましょう。また外部にプログラムやIT機器の開発を委託する場合、詳細が開示されないうちに、情報の取扱が厳密でない外国に対して、「オフショア開発」で業務が再委託される場合があります。こういった場合、発注者のあずかり知らぬ所で、情報漏えいやシステム上にバックドアを仕込まれてしまう可能性があります。そのようなことを防ぐため、契約時には禁止行為や監査などを取り決めましょう。



## 6.2 問題が起きると事業継続に影響を及ぼす

攻撃者によるサイバー攻撃だけでなく、十分に気を付けなければならないのは内部の人間、およびそれに準じる人間によるサイバー犯罪です。

現実にあった例を下敷きに説明しましょう。

とある会社で営業機密や顧客情報の流出が発覚しました。その犯人は過去にその会社に在籍していた人物で、とくに複雑なハッキングをせず、在籍時のアカウントを使ってアクセスし、情報を抜き取ったのでした。

退職者のアカウント管理をきちんと行っていなかったために発生したケースと言えます。

また、回線を使った侵入すら行わないケースもあります。

とあるサービス業から顧客情報が約数百万件流出するという事件が発覚しました。

その会社自身が流出に気付いたものではなく、流出した名簿を使って顧客にダイレクトメールが届くようになったことで、間接的に数百万件の顧客情報流出が発覚したものです。

情報流出は親会社から業務委託された情報処理系の子会社から、外部の派遣社員のエンジニアが顧客データを持ち出し、名簿業者に不正に転売した結果起きたものでした。

本件は、クラッキングなどを行ったサイバー攻撃によるものではありませんが、内部犯行者によるれっきとしたサイバー攻撃でした。

これにより親会社は顧客に数百億円相当の補償を行い、また、子会社は事業継続が困難となって翌年に解散。犯人は当然のことながら逮捕、責任を負うべき立場にいた役員が引

### 受託事業の機密情報を流出させてしまった



受託事業で預かった機密情報や個人情報▶用語集 P.196 など、IT 機器を導入していると、目立たずあっという間に持ち出されたり、流出してしまったりします。上記のイラストでは、外部から来た派遣社員の例ですが、ソーシャルエンジニアリングを使って会社に入り込んだり、社員を騙して送らせたり、あるいは外部からサイバー攻撃を行い社内や団体内のコンピュータなどを乗っ取って流出させたり、その可能性はいくらでもあります。こういったトラブルが発生したとき、相手先や顧客への不利益はもちろん、会社として受ける損害は計り知れません。

### なぜこれがサイバー攻撃なのか？



誰でもさわれるPCに入ればなし パッチあてずにつなぎっぱなし

外部の人間が機密情報の入ったパソコンに、USB メモリを挿して情報をコピーして持ち出した。ネットワーク越しに受けるサイバー攻撃だけでなく、こういった物理的な盗難も広義のサイバー攻撃です。サイバー攻撃とはネット経由に限らず現実世界も含むのです。

盗難されたデータはその先で、また、別のサイバー攻撃を生みます。例えば盗んだ名簿が現実世界の名簿屋やダークウェブ▶用語集 P.198 上のダークマーケットで販売されると、その名簿を買った別の攻撃者が、スパムメール▶用語集 P.197 などを使ったサイバー攻撃に用いる可能性があるのです。

責辞任となりました。

このケースでは親会社と子会社の関係でしたが、これが資本関係のない契約企業だった場合、損害賠償請求が行われたかも知れません。

ましてやこれが、社員数名しかいない中小組織だったら、金銭的賠償

は不可能でしょうし、NPO だった場合は、高い意識を持って始めた事業であっても、情報流出を起こしたことで信頼を失い、その目的の達成を断念せざるを得ない事態に陥ったでしょう。

# 企業が気を付けたいサイバー攻撃の具体例を知ろう

## 7.1 標的型メール攻撃の具体例

「お盆休み明けに出社して、すぐにメールを開くと、提携先の会社のAさんから、次回のミーティングに関するレジュメが添付されてきていた。ミーティングは当分先だったのではと思いつつ、このファイルをクリックして開いたが、レジュメは表示されなかった。ファイルが壊れているのかな…。まあいいか。」

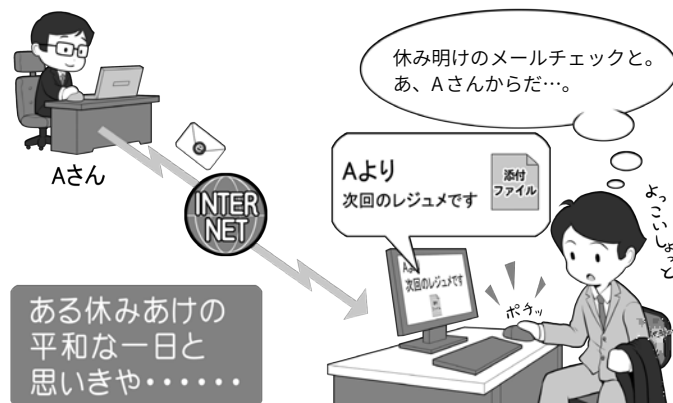
はい。アウトです。こんな話は、どこの会社や団体でも見るありふれた光景でしょう。しかし、この話には3つのポイントがあります。

1つは、長い連休中にはセキュリティアップデートや、総合セキュリティソフトの更新が行われている可能性があります。日常的な業務を始める前に、まずアップデートして連休中に見つかったシステムのセキュリティホールや新しいマルウェアに対応できる状態にしましょう。

2つめに、どこかの会社のAさんが、本当にAさんか確かめるのは、ややレベルが高いとしても、少なくともこの時期にAさんからメールが来たことに疑問を持っています。そういうときは連休中にAさんのメールが乗っ取られた可能性を考えて、メールではない手段(電話やビジネスチャットなど)でAさんに添付ファイル付きのメールを送ったか確認しましょう。

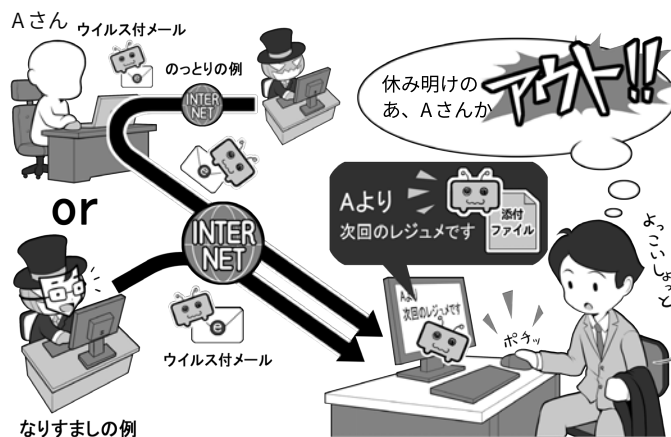
3つめ、添付されているファイルをいきなり開き、きちんと見られなかった点で、マルウェアの可能性を

### こんなシチュエーションだと思っていたら…



休み明けに出社して、普段どおりにパソコンを立ち上げ、メールを開いて読む。しかし、この一連の流れには攻撃に対する視点が欠けています。攻撃者だったらどう攻撃するかという視点です。休み明けということは、何日間かパソコンを立ち上げていない時間が存在し…

### 実はこんなシチュエーションかも…



その間には、新たなセキュリティホールが発見され、攻撃者が攻撃するためのマルウェアを開発して、取引相手になりすましたり、アカウントを乗っ取ったりして、そのマルウェアを送ってきているかも。標的型メール▶用語集 P.201 に対処するには、メールを開く前にまず、アップデートしてシステムを最新の状態にします。

考えていません。ひらけなければ疑問を持つべきですし、開いた場合でもなにかをインストール▶用語集 P.194 しろとか、あなたに許可を求めるものは、総じて疑うべきです。

それに原則的なルールは、「メールを見ただけで完結しないものはす

べて疑え」であり、「挙動が怪しい場合には、組織内にセキュリティ担当の窓口が設置されていれば、そちらに連絡する」です。それは添付ファイルでもメールの文中の外部ウェブサイトへのリンクでも同じです。

## 7.2 フィッシング攻撃の傾向

「オンラインショッピングの会社からメールで、『あなたのアカウントが攻撃され、一時的に利用停止になった。下記からログインして、停止を解除して下さい』という内容のものが送られてきた。リンクを開くといつもどおりのそのショッピングサイトのロゴとデザインのウェブサイトが表示されたので、IDとパスワードを入力して、停止を解除した。」

あなた宛に名指しで送られてくるメールなどと違い、個人名がなく不特定多数に送られることが多いのが、ばらまき型のフィッシングメールです。余談ですがフィッシングとは釣り Fishingではなく、詐欺の意味の Phishing から来ています。

上記の話は有名なもので知っている方も多いと思いますが、ねつ造された偽物のウェブサイトは、最近では本物と見分けが付きません。

あなたがIDとパスワードを入力すると、それをだまし取って勝手にオンラインショッピングサイトで買い物をし、商品を転売するなどしてお金を手に入れるわけです。

このメールも文面を見ただけで完結しないので疑うべきです。

なお、こういった警告が来た場合、メールのリンクは使用せず、ウェブブラウザで検索し直接そのショッピングサイトなどを訪れてみて下さい。本当にアカウントが停止されているならば、警告が表示されるでしょう。

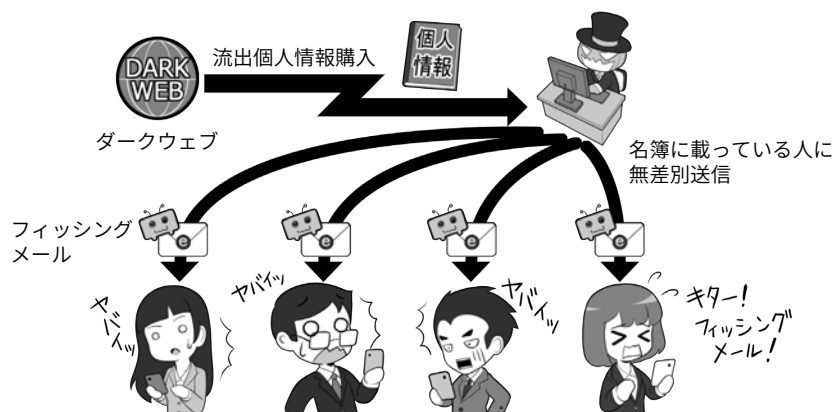
一方で、そのウェブサイトがショッピングサイト相当の暗号化(https://  
▶用語集 P.191)に対応していて、一見そのショッピングサイトと同じ名前を掲示していても、実は「アルファベットに似た別の言語の文字」を使用し

### すぐに対処しようと思ったら…



SMS ▶ 用語集 P.192 やメールで「パスワードが流出しました。至急変更を!」という連絡がきても、ちょっと待ちましょう。それは本当に自分が使っているサービスから送られてきていますか?

### 実際はこういうワナだった!



攻撃者はどこかのウェブサービスなどから流出したメールアドレスなどを買って、IDとパスワードを盗む攻撃をしかけてきます。反応するとアカウントを乗っ取られるかも。

### それには解りにくくなる工夫も



メールのリンクを開いて、飛んだ先のウェブサイトがそのサービスの本物のページとは限りません。似たような単語を使った別のウェブサイトの場合もあるのです。よく確認しましょう。

ている場合もあります。

具体的にはロシア語などで使われるキリル文字は、アルファベットと似た字形のものがあありますが、イン

ターネットでは別の文字として扱われるので、同じに URL ▶ 用語集 P.193 に見えて別のウェブサイトを作れるのです。



## 7.3 不正アクセスの傾向

「ある朝、会社に出社したら、取引先から『お宅に渡した当社の機密情報がネットで公開されているじゃないか、どういうことだ!』というクレームの電話が来ていました。それを受けて調べるみると、社員で共有に使っていた社外のクラウドストレージサービスのIDとパスワードが何者かに破られて、社外からアクセスをされ、情報が流出していました……。でもなぜIDとパスワードが漏れたんでしょう…」

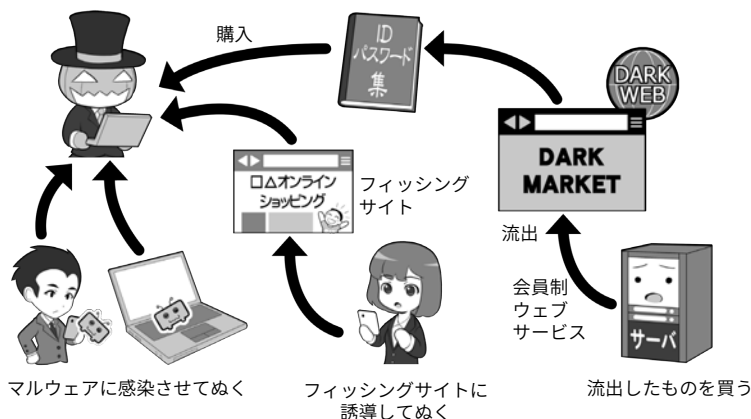
この問題は複合的で、「①なぜIDとパスワードが漏れたのか」だけでなく、「②なぜ漏れたIDとパスワードでクラウドストレージサービスにアクセスできたのか」、最後に「③なぜクラウドストレージサービスから情報流出を許してしまったのか」の要素があります。

①のIDとパスワードの流出はマルウェアの感染やウェブサービスからの流出などがあり、自分で防げるものと防げないものがあります。自分で防ぐには、セキュリティをきちんと固めるだけです。一方、ウェブサービスからの流出は、多要素認証▶用語集 P.198を導入していないセキュリティ意識が低いサービスを避けるなど、消極的手段はありますが、最終的には自分でどうにかすることはできません。

どうにかできないをカバーするには、②のなぜクラウドにアクセスできたかの問題ごと封じます。この場合は個人と業務用でパスワードの使い回し▶用語集 P.201をしていたことが原因なのでこれを防ぐのです。たとえば漏れても被害が発生しないようにするには、1つはパスワードの使い

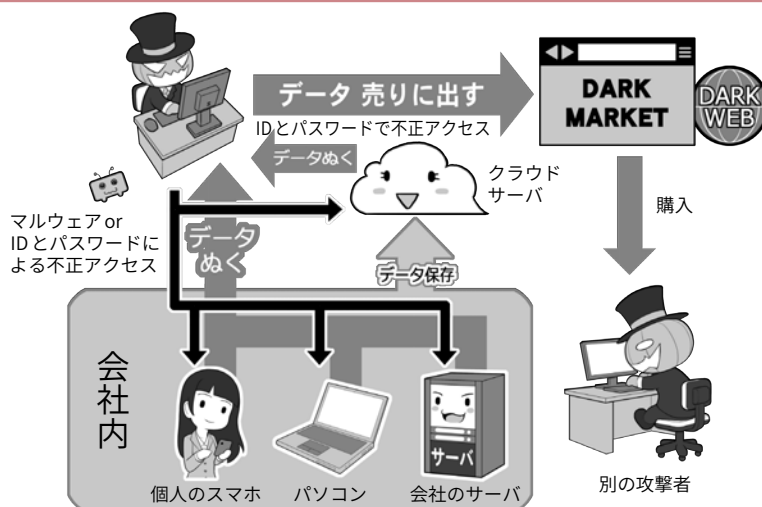
### 不正アクセスを行うために攻撃者は…

#### ①IDとパスワードを狙う



攻撃者は不正アクセス▶用語集 P.202を行うために、IDとパスワードを収集します。前ページのように偽のウェブサイトへ誘導して抜く方法以外にも、マルウェアに感染させて抜く、流出した情報をダークウェブにあるマーケットで購入して集めるなど、さまざまな手法があります。それを使って別のウェブサービスや業務上のサービスに不正アクセスを行おうとします。このとき、IDとパスワードの使い回しをしていると、侵入されてしまう危険性が跳ね上がります。

#### ②データを狙う



不正アクセスができれば、今度はあなたが持っている機器、使っている機器から情報を抜き取ります。それをダークウェブのマーケットを経由して誰かに販売するかもしれません。クラウドサーバ上にあるデータも、アカウントを盗まればアクセスされて、保管しているデータを盗まれるでしょう。盗まれたデータが受託した業務に関連するものだった場合、自社だけでなく発注元企業に被害が及び、また個人情報だった場合、顧客などに不利益を与える結果になります。アカウント情報を盗まれないように、細心の注意を払いましょう。

回しを絶対にしないこと。もう1つは、多要素認証を導入して、漏れてもIDとパスワードだけではアクセスできないようにすることです。

③でさらにクラウドにアクセスを許しても情報流出を許さないためには、アクセスできる人間を限定する

ことや、重要情報を見られる人間を共有設定で限定すること、そして、機密情報などは例えファイルとして流出しても、その内容を閲覧できないように、ファイルごとに暗号化を施すことです。



## 7.4 不正送金の傾向

お金を直接狙うサイバー攻撃は、取引先のふりをして振り込み口座を変更させるBEC▶用語集P.190や、不審なメールやメッセージから銀行にそっくりのウェブサイトに誘導して、IDとパスワードを抜いたり、実際にインターネット上で送金するとき、その通信の間に割り込んで、目的の口座に振り込ませる「中間者攻撃」▶用語集P.199と呼ばれるものなどがあります。

警察庁の発表によれば、令和元年の発生件数1872件、被害総額25億2100万円をピークに発生件数、被害総額ともに減少していましたが、令和4年は、発生件数、被害額ともに増加に転じています。また、その手口の多くはフィッシングによるものとみられています。

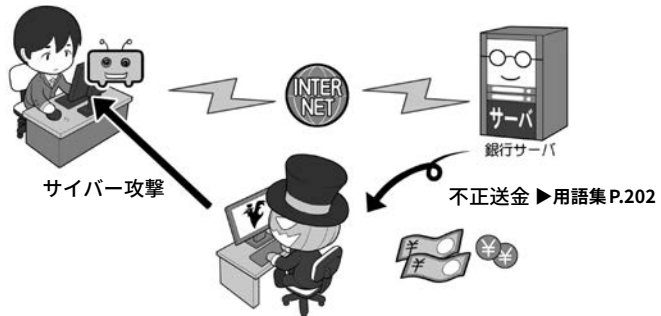
「会社の口座を確認したら、空になっていた。」こうなってしまった場合は回収できたとしても時間を要するでしょう。会社の運転資金までやられてしまえば、事業継続は困難になります。

幸いにして情報の流出などと異なり、銀行の場合は過失が無いことが認められれば、銀行側が補填してくれることもあります。クレジットカードの不正利用なども同様です。

一方、場合によっては補填が行われないのが、暗号資産を奪取する詐欺です。暗号資産は通貨といいながら、平たくいえば暗号化された情報なため、不特定多数をフィッシングメールでマルウェアに感染させ、情報を奪取することも行われています。

これらに対処する特別な方法はなく、今までの3項目であるような基本的な対処方法と、もう1つは同様

### オンライン決済は常に狙われている



オンラインの銀行決済は常に狙われています。取引先になりすましてBECだけで誤った口座に送金させる手口や、偽サイトでIDやパスワードを奪う方法、そしてなんらかの手段で決済の間に割り込んで振込先を自分の口座にすり替えてしまう中間者攻撃。

多要素認証、パスワードなどの厳重保管、BECやフィッシングメールに騙されないスキル、そして総合セキュリティソフトなどを導入している場合は、決済専用のブラウザを使うなどの防御手段があります。

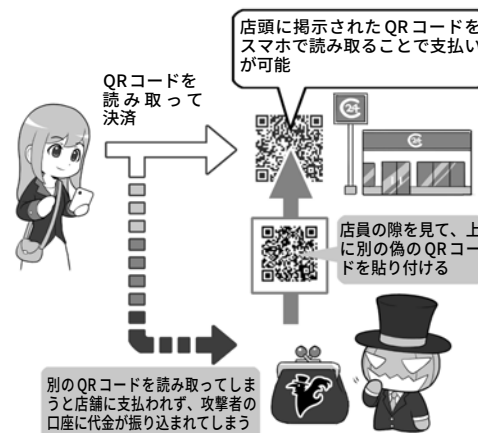
### 犯罪者に狙われる暗号資産



暗号資産を巡るサイバー攻撃も続発しています。実際、国内外含め多くの暗号資産取引所がサイバー攻撃を受け、大きな金銭的被害が生じた事例がある他、暗号資産の窃取を目的としたマルウェアも登場しています。

暗号資産をネタにした投資詐欺▶用語集P.199が増えています。どのようなものであっても「必ず儲かる」という話はありえませんが、くれぐれもご注意ください。

### QRコード決済▶用語集P.191の詐欺の流れ



まず犯罪者が店舗に掲示されたQRコードの上に、別のQRコードを貼り付けます。利用者がそのQRコードを使って決済を行うと、代金は店主ではなく犯罪者の口座に振り込まれてしまうという流れです。

の手口の情報を、アンテナを高くしニュースやネットの記事、SNSなどから集めて、いざ攻撃されたときに、「似たような話を聞いたことがある。

不信だ」と気付くようになることです。

なお、不正送金が疑われる事象があった場合は、速やかに銀行やクレジットカード会社に相談しましょう。

## 7.5 ランサムウェアの傾向

「始業時間に会社に来てパソコンを起動すると、『このパソコンは乗っ取った。データはすべて暗号化したから、データを返して欲しければ身代金を払え』というメッセージが出て、送金期限までのカウントダウンが始まった……」

これがランサムウェア(ランサム＝身代金)▶用語集 P.203 と呼ばれるマルウェアの典型的な手口です。

ランサムウェアへの対処方法は、システムを常に最新の状態に保つことと、仮に攻撃されても、組織としての対応方針をあらかじめ策定し、感染したシステムを初期化▶用語集 P.197 しバックアップから復旧できる体制を整えることです。感染しにくくするためには、とくに外部からアクセス可能な機器について、地道にセキュ

### ランサムウェア感染はビジネスにも影響



ランサムウェアはパソコンなどの中のパイルを勝手に暗号化するため、感染すれば仕事上の極めて重要なファイルも人質に取られてしまいます。大事なデータが入ったパソコンが使えなくなれば、業務停止、納期遅延など顧客に迷惑をかけ、その結果、会社としての信用を失う恐れもあります。バックアップは常にしておきましょう。

リティ対策を施していく必要があります。

身代金を支払ってもデータが復元

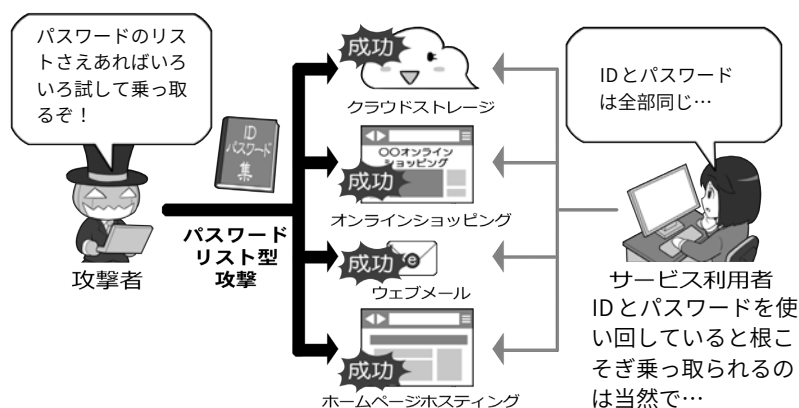
▶用語集 P.202 される保証はないですし、攻撃者を助長するだけなので避けましょう。

## 7.6 ウェブサービスへの不正ログイン

先ほどの情報流出の件でも登場しましたが、クラウドストレージサービス、オンラインショッピング、メール、ウェブサイト運用など、ウェブサービスと総称されるインターネットのサービスは、常に攻撃者からの乗っ取りの危険にさらされています。常にこれを阻むことを考えましょう。

IDやパスワードの使い回しをしないことと、さらにサービスを利用する際に、多要素認証などやUSBセキュリティキー▶用語集 P.193 などを用いて、攻撃者が不正ログイン▶用語集 P.202 しにくくなる環境を整備しておきましょう。

### パスワードを使い回しをしていると攻撃に

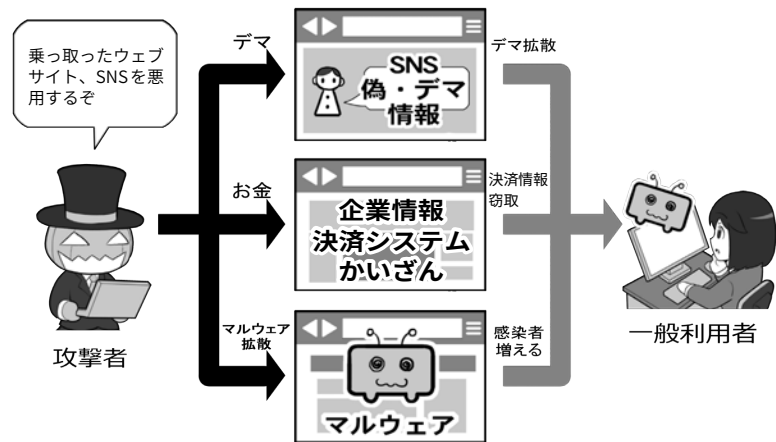


つい面倒くさがってIDとパスワードを使い回ししていると、どこか1つでも流出が起これば、同じIDとパスワードを使用しているサービスが根こそぎ乗っ取られる場合があります。また、別々のパスワードを使っている、そのパスワードがよく使われるような簡単なものだった場合、そういったパスワードをまとめたリストが流通していて、それを使ってアカウントを乗っ取る攻撃が行われます。一部を変えただけなど、似たようなパスワードも非常に危険です。

## 7.7 ウェブサイトの改ざんやSNSの乗っ取り

会社や団体のウェブサイトは、ホスティングサービス▶用語集 P.203 と呼ばれる、専用の業者のサーバを利用していることも多いと思います。これらのサービスはセキュリティを自分で管理する代わりに、ホスティングサービスに外注している形になり、特殊なカスタマイズを施さなければある程度のセキュリティは確保されています。一方、管理者アカウント情報を推測されたり、ウェブサイトなどの脆弱性▶用語集 P.197 を突かれたりして不正アクセスされ乗っ取られると、改ざんされ偽の情報を発信したり、マルウェアなどを埋め込まれ、不特定多数にサイバー攻撃をしてしまったりします。認証情報はきちんと管理し、多要素認証などで容易に

### ウェブサイトに乗っ取られると攻撃の拠点に



管理者アカウント情報を推測されたり、ウェブサイトなどの脆弱性を突かれたりして不正アクセスされ、自社や団体のウェブサイトを運用しているサーバが乗っ取られると、攻撃者はそのウェブサイトを使ってサイバー攻撃を行います。  
例えば偽の情報を発信する、公開されている企業の情報を改ざんする、あるいはそのウェブサイト自身をマルウェアの発信元にして、ウェブサイトを訪問した人のIT機器をマルウェアに感染させ、乗っ取ったIT機器をどんどん増やしていくかもしれません。  
一方、WordPressなどのウェブサイト作成ソフトは、それ自身をアップデートしないで使用すると、発見されたセキュリティホールを悪用されるので、きちんとアップデートしましょう。

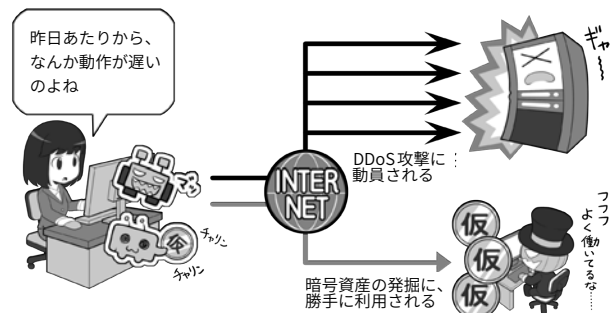
不正アクセスできないように設定し しましょう。

## 7.8 DDoS攻撃

DDoS攻撃▶用語集 P.190 とは、複数のIT機器からウェブサーバに対して大量のデータを送りつけて応答不能にするサイバー攻撃です。DDoS攻撃を受けると、利用しているインターネットサービス、いずれもが処理能力オーバーで機能しなくなり、ウェブサイトならばアクセスできなくなります。これに関してはウェブサーバ側で対処できることが少ないのが実状です。事前にCDN(Content Delivery Network)▶用語集 P.190 サービスを利用するようにしておけば、DDoS攻撃をある程度緩和できる可能性があります。

一方、自分の会社や団体のIT機器などが乗っ取られDDoS攻撃に利用されている場合は、利用停止、ネッ

### 乗っ取ったIT機器は直接的サイバー攻撃などに



マルウェアに感染させられたIT機器は、自分が被害に遭うだけに留まらず、他のIT機器やサーバに対して直接的なサイバー攻撃に駆り出されることもあります。例えば不正な情報リクエストを集中させ、相手のサーバが反応できない状態に追い込むDDoS攻撃などを行います。また、IT機器の動作がおかしいときには、気付かないうちに暗号資産の発掘に利用されている場合もあります。普段と比べて動作が遅い、不審な挙動をするなどといったときは注意しましょう。

ト切断、通報の判断、周りを含めマルウェアの駆除、バックアップからの復旧などをする必要があります。  
DDoS攻撃に限らず、総合セキュリティソフトが反応しない場合、マ

ルウェアの感染を検知するのは、「なか動作が遅い。おかしい」といった、正常動作時との差なので、そういった点にも気を配りましょう。



## 7.9 サイバーセキュリティ以前の情報モラル教育を怠らない

顧客情報を狙う攻撃者の視点から、情報を手に入れる手段を考えると、狙った社員の心隙を突くソーシャルエンジニアリング方法などが考えられます。例えばSNSで相手を見つけて「名簿高く買うよ」とそそのかす方法などが考えられます。

ただ、情報流出が起こるのは狙われたケースだけではありません。「列車内に鞆ごとパソコンを置き忘れる」「顧客情報の入ったUSBメモリを落とす」「車内に置き忘れた生徒の成績表の入った記憶装置▶用語集P.195を盗まれる」「全顧客にメールを送信しようとしたら全顧客の宛名が見える形で送信してしまった」など顧客情報の流出の報道は枚挙に遑がありません。

「それってサイバー攻撃なの？」といわれれば、直接的にはサイバー攻撃ではないかもしれませんが、しかし、流出したものがダークウェブなどで販売されれば、サイバー攻撃につながります。

こういった内部犯行や情報流出を防ぐには、防御手段をとった上で情報モラル教育▶用語集P.197をきっちり行うことです。

例えば内部犯行防止に、必要がないときに顧客情報を扱う部屋に人を入れないよう、部屋や建物に施錠をしているのでしょうか。アルバイトや社員に、きちんと情報モラル教育をしているのでしょうか。

あるいは、仮に置き忘れや紛失、盗難が起こってしまっても、完全な情報流出が起こらないようにするリカバリ手段を講じたり、問題が起こったらどう対処するか、その段取りを考え訓練したりしているのでしょうか。

### 情報流出の可能性はたくさんある



流出の可能性は情報を扱う人を狙ってそのかすことだけではありません。機密情報を入れたパソコンをカバンごと電車やタクシーの中に置き忘れる、生徒の成績などが入ったUSBメモリを落とす、多数の人に一斉メールを送ろうとしたら、互いのメールアドレスが分からないBCC欄ではなく、見えてしまうTOやCC欄に入れて送信してしまった、などなど。パソコンやスマホ、IT機器は便利な反面、ミスを犯すときも一瞬で多量に失います。要注意です。

### サイバーセキュリティにつながる予防策



内蔵記憶装置  
暗号化

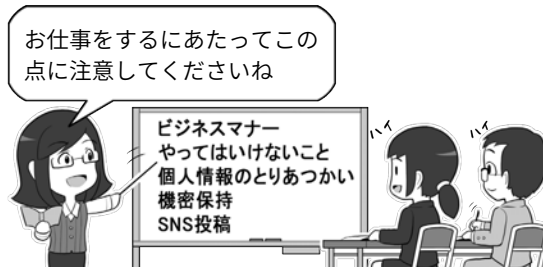
暗号化  
USBメモリ

資格のない人には  
さわせない共有設定

必要ない人が  
立ち入らないように施錠

現実世界、ネットの世界、両者に共通する情報流出の防御手段は、機密情報を扱うパソコンや記録媒体は暗号化した上で、その部屋や建物には必要がない人が入れないようにすること、施錠をきちんと行うこと、パソコンなども使用しない場合はロッカーにしまって鍵をかけること、ハッキングを受けないようにネットワークには接続せずにスタンドアロン▶用語集P.197で使用すること、使用できる人の資格設定をきちんと行い、資格がない人には触れないようにすることなど、できる事はたくさんあります。

### 大切なのは情報モラル教育



お仕事をするにあたってこの  
点に注意してくださいね

こう言った機器やシステムの防御策だけでなく、同等に大切なのは、情報に触れる社員や会員に対する情報モラル教育です。機密情報の取扱だけでなく、最近ネットを賑わせる、問題のあるSNS投稿などを起こさないように、ネットリテラシーを含んだ勉強会や教育を行う事が、求められています。

情報流出というと、攻撃事例だけに注目をしてしまいがちですが、他にも情報流出は起こりえますし、一方で情報管理の基礎を守ればそれらを防ぎ、被害を抑え込むリカバリ手

段も打てるのです。

そういったサイバー攻撃以前の備えの必要性を忘れないようにした上で、一般的なサイバー攻撃の事例を知りましょう。



# 個人情報情報は法律に則り適切に取り扱おう

個人情報の取扱に関することは、「負のコスト」を発生させないための重要な要素です。

個人情報保護法は、中小組織あるいは町内会・自治会、学校の同窓会などにも適用され、個人情報を取り扱う際のルールとして、その遵守が求められています。

個人情報保護法では、個人データを第三者に提供する場合、本人の同意を得る必要があります(第27条)。また、国外に個人データを移転する場合にも原則として本人の同意が必要とされる他(第28条)、令和4年4月の法改正により、外国にある第三者への個人データの提供時に、提供先の第三者における個人情報の取扱に関し本人に対して詳細な情報提供が求められるようになりました。外国に設置しているサーバーで個人データを取り扱う場合などは、当該外国の個人情報の保護に関する制度などを把握した上で安全管理措置を講じる必要があります。

個人情報保護法に違反しますと、個人情報保護委員会▶用語集 P.196 から指導などを受け、会社の社会的信用を損なう可能性があります。

個人情報の適切な取扱に関し、個人情報保護委員会では、「はじめての個人情報保護～シンプルレッスン～」として、「中小企業向け『これだけは!』10のチェックリスト」を公開しています。

その中で、パソコンでのデータの保管は、システムを最新に保つ、セキュリティソフトを入れる、ログインパスワード▶用語集 P.204 の設定や

## 気を付けたい個人情報の取扱

### 巻末資料 中小企業向け基本の10のチェックリスト

分類	No.	チェック項目	ポイント	関連ページ
取得・利用	<input type="checkbox"/> 1	取り扱っている個人情報について、利用目的を決めていますか？	目的は具体的に。 ○「新商品のご案内の送付のため」 ×「当社の事業のため」	P3
	<input type="checkbox"/> 2	その利用目的は、本人に通知するか公表していますか？	取得の状況からみて利用目的が明らかなら通知・公表は不要。	P3
保管・管理	<input type="checkbox"/> 3	(組織的の安全管理措置) 個人情報の取扱いのルールや責任者を決めていますか？	個人情報の保管場所や漏えい等発生時の社内の報告先は決まっていますか？	P4~6
	<input type="checkbox"/> 4	(人的安全管理措置・従業員監督) 個人情報の取扱いについて従業員に教育を行っていますか？	個人情報の保管場所等のルールは周知できていますか？	P4~6
	<input type="checkbox"/> 5	(物理的の安全管理措置) 個人情報が含まれる書類や電子媒体について、誰でも見られる場所・盗まれやすい場所に放置していませんか？	不要になった情報は適切に廃棄・削除することも大切。	P4~6
	<input type="checkbox"/> 6	(技術的の安全管理措置) パソコン等で個人情報を取り扱う場合、セキュリティ対策ソフトウェア等をインストールして最新の状態にしていますか？	ログイン時にパスワードを要求したり、ファイルにパスワードをかけることも大切。	P4~6
	<input type="checkbox"/> 7	個人情報の取扱いを委託する場合、契約を締結する等、委託先に適切な管理を求めていますか？	委託先にも安全管理を徹底してもらうということ。	P4~6
第三者提供	<input type="checkbox"/> 8	本人以外に個人情報を提供する場合、本人に同意をとっていますか？	法令に基づく場合(警察や裁判所からの照会等)や、委託に伴う提供には同意不要。	P7・8
	<input type="checkbox"/> 9	本人以外に個人情報を提供したり、本人以外から個人情報を受け取る際、相手方や提供年月日等について記録を残していますか？	法令に基づく場合(警察や裁判所からの照会等)や、委託に伴う提供には記録不要。	P7・8
開示請求等	<input type="checkbox"/> 10	本人から自分の個人情報を見せてほしいと言われたり、訂正してほしいと言われた際には、対応していますか？	開示等の請求に対応する人は決まっていますか？	P9~10

※このチェックリストは、主に中小企業を対象に、個人情報保護法を遵守できているかどうかを確認する際の参考に作成したもので、これ以外にも留意すべき事項があります。個人情報保護法のルールの詳細は、本シンプルレッスンの関連ページや、個人情報保護委員会のHP等をご参照ください。

出典：個人情報保護委員会ウェブサイトより [https://www.ppc.go.jp/files/pdf/simple\\_lesson\\_2022.pdf](https://www.ppc.go.jp/files/pdf/simple_lesson_2022.pdf)

データを暗号化するという事項が掲載されています。より安全に保護するためには、個人情報を取り扱うパソコンを明確にし、不必要にネットにつなげないようにすることの他、USBメモリを使ってデータを抜き出すことができないようにすることが必要です。

また、使用していないときは、個人情報を記録したパソコン、もしくはデータが自動的に暗号化される外付け記憶装置を使っている場合はそれを、物理的に鍵がかかるロッカーなどに保管して、流出事故を起こして完全なる負のコストを発生させないようにしましょう。

# フリー素材の取扱と著作権について注意しよう

インターネット上の素材を利用する上で、知っておくべき概念として、いわゆる「フリー素材」とよばれているものがあります。

「フリー」といっても「著作権を放棄しているので勝手に使ってよい」ということではなく、「著作権者の厚意で、一定の条件の下に、無料で利用することが許されている」という意味なので注意しましょう。

この点を理解せず、利用条件をよく確認しないままコンテンツを勝手に使ってしまうと、著作権侵害▶用語集 P.199 をしているとして、炎上したり、著作権者から損害賠償を請求されたりするなど、不必要な負のコストを生んでしまうことになります。

一口に「コンテンツ」といっても、その中身はプログラムや画像、映像、動画、音、音楽など多岐にわたり、コンテンツの種類によって利用条件が異なる場合があります。また、著作権者が認めている利用条件の内容も、完全な著作権フリー（著作権を放棄または一切行使するつもりはないため、著作者の明示も要求されず、用途も営利・非営利を問わず利用可能で、改変も許される）といったものから、著作者名は明記しなければならないもの、非営利目的での利用のみが許されるもの、改変が許されるもの・許されないもの、など、さまざまな条件があります。また、中には著作権の保護期間が満了したためパブリックドメイン(PD)となり、基本的に自由に利用できるものもあります。

## クリエイティブ・コモンズ・ライセンスとは

すべての著作物には著作権があり、著作権は守られなければなりません。インターネットには著作権者によって「条件を満たせば比較的自由に使ってよい」とされているコンテンツが多く存在します。クリエイティブ・コモンズは、そのルールを簡単に示すための試みとして、クリエイティブ・コモンズという国際的非営利組織とそのプロジェクトによるクリエイティブ・コモンズ・ライセンスがあります。

クリエイティブ・コモンズ・ライセンスでは、その条件をわかりやすくするために特定の条件に関するマークを定めています。



参考：クリエイティブ・コモンズ・ジャパン ウェブサイト

<https://creativecommons.jp/>

クリエイティブ・コモンズに関して、詳しくは上記ページを参照してください。

## 無断使用は著作権侵害で賠償も



インターネットでは「パクリ」▶用語集 P.200 と呼ばれる著作物の無断使用が散見されます。無断で使ってもばれないだろうといった軽い気持ちで使っているのでしょうか。しかし、私たちが普段インターネットの検索エンジンを使って、世界中のウェブサイトにある情報を検索できるように、画像などが使われている場所も検索できるので、他人の著作物を勝手に使った場合、それが判明してしまいます。そもそも、著作物を著作権者の許諾なく勝手に利用する行為は、著作権法に違反し、著作権者から無断使用に対する損害賠償請求を受ける可能性があります。きちんと著作権者の許諾を得てから利用するか、利用条件が明示されているコンテンツをその条件にしたがって使いましょう。

このようなコンテンツの利用条件を簡単に示すものとして、「クリエイティブ・コモンズ・ライセンス」がよく使われています。

クリエイティブ・コモンズ・ライセンスではそれぞれ「どう使ってよいか」が、マークなどで明記されているので、その範囲で活用させてもらいましょう。

コンテンツの利用を許諾している著作権者の中には、自分のコンテンツをどこで使ったか教えて欲しいという方もいるので、その場合は、どこで使ったかを報告するとともにコンテンツを使わせてもらった感謝を伝えましょう。

著作権には保護期間があり、すでに述べたとおりこれを過ぎると基本的には自由に使うことができますが、個人が著作権者である著作物の保護期間は著作権者が亡くなってから70年なので、いつ保護期間が終わったのか簡単に分からない場合もある点に注意が必要です。

また、自社のウェブサイトで、写真を利用したい場合などとも思いますが、写真などを利用する場合には、写真そのものの著作権だけではなく、被写体の権利にも注意する必要があります。例えば、人物を撮影した写真の場合には、被写体となっている人には肖像権があります。ですので、写真を撮影した人(＝写真の著作権者)から、写真を利用することについて許諾をもらっていたとしても、写っている人から「ダメ」と言われたら、その写真を使うことはできません。また、その写真に、絵画などの別の著作物が写っている写真を使おうとする場合には、原則その絵画の著作権者からの許諾も必要となります。したがって、写真やイラストなどを使おうとする場合に

## 写真の著作権と被写体の権利の両方に注意しよう



自社サイトの広告や記事などを作るとき、「写真を掲載したい」と感じることはよくあるでしょう。その際、写真には、写真そのものの著作権だけではなく、被写体の権利にも注意する必要があります。写真を撮影した人(＝写真の著作権者)から、写真を利用することについて許諾をもらっていたとしても、肖像権のある被写体である人から「ダメ」と言われたら、その写真を使うことはできません。写真については、「ストックフォト」など、被写体の権利について明記したサービスなどもあるので、目的に応じて使いやすいものを選びましょう。

は、その写真やイラストの著作権者の許諾だけではなく、被写体(描写されている人・物)についての許諾があるかどうかを確認する必要があります。

ネット上で見つけた写真を利用する場合には、そのような被写体の権利についても配慮し、例えば、被写体の人物からの許諾がきちんと得られているのか、または人物が特定できないようになっており被写体である人からの許諾なく使用してもよいものなのか、などについても確認してから利用するようにしましょう。

写真のコンテンツに関しては、「ストックフォト」といわれる写真素材

があります。「ストックフォト」は、特定のシチュエーションでの使用が想定された写真素材では、被写体についての許諾のあり／なしが明示されている場合があります。ウェブ上で自社を紹介する広告や記事などを作りたいときに写真が必要になったら、許諾があることを明示された写真を選ぶとよいでしょう。ちなみに、ストックフォトは有償無償さまざまなサービスがありますが、被写体についての許諾は、人物の場合は「モデルリリース」、物の場合は「プロパティリリース」などという表記が使われているケースをよく見かけます。



## 取引先の監督を徹底しよう

自社のセキュリティは十分に高度にしていたのに、大事なデータを渡していた関連会社や取引先がずさんな管理を行っていて、個人情報を流出させてしまった……。

そんなとき「関連会社がやったから……」といったとしても国民や社会の理解を得ることができないのは、これまでの情報流出の事例を見ても明らかです。

自社が持っている個人データの取扱を利用目的の達成に必要な範囲内において委託し、それに伴って取引先に当該個人データを提供する場合には、本人の同意に基づき取引先に提供する場合と異なり、記録義務はありません。しかし、その一方で取引先を監督する義務を負います。

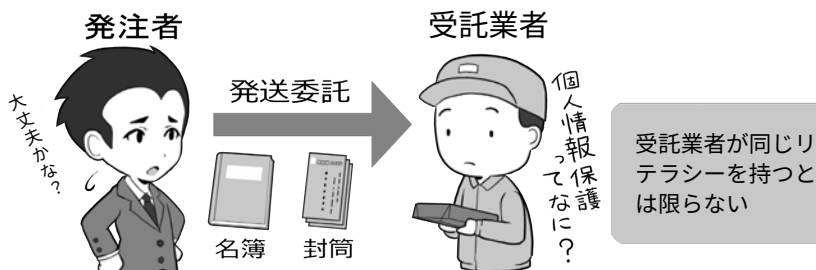
具体的には

1. プライバシーマークを取得するなど、きちんと個人情報を取り扱える能力のある業者を選定すること
2. 取扱の内容を契約書に明記すること
3. 契約の内容が守られているか定期的に監査すること
4. 業務委託先が外国に設置したサーバーで顧客データを取り扱う場合は、どのような安全管理措置が講じられているかについて明示して監査すること

が義務づけられます。

詳しくは個人情報保護委員会のウェブサイトなどを参照して欲しいのですが、こういったことをきちんと行うことが、個人情報を厳密に扱う姿勢を委託先に示すことになり、不正な個人情報の流出への抑止力にな

## 取引先が自分と同じリテラシーを持つとは…



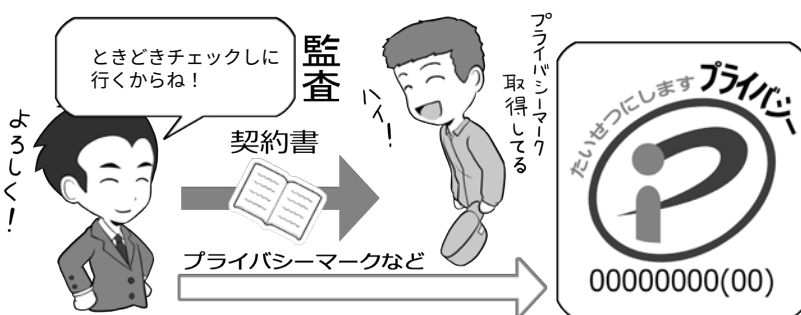
個人情報やプライバシーに関して、きちんと管理しなければならないことであるという意識は広がっていますが、それは自社や自団体の中だけにはなっていませんか？

その意識は取引先や委託先まで徹底されてるのでしょうか？

自社や自団体と委託先は別ではなくて、例えば宛名を渡して発送業務を行う場合でも、その個人情報にまつわる監督責任が発生します。また、委託先が自社や自団体と同じリテラシーを持つと安易に考えないで、確認を怠らないようにしましょう。

専門性のある委託先に業務をアウトソースしてコストを抑えるのはよいことですが、抑えるべきポイントは抑えましょう。

## 自分たちも相手もトラブルにならないために



個人データを取り扱う業務を委託する場合は、委託先を監督する義務が発生し、プライバシーマークを取得しているかなど適切な取扱の体制が整備されているかを確認し、個人データの取扱に関して契約書に明記し、その内容が守られているか定期的に監査するなどの対応が必要となります。

なお、プライバシーマークに関しては一般財団法人日本情報経済社会推進協会 (JIPDEC) のウェブサイトの、プライバシーマーク制度のページに詳しく記載されているので、参照してみてください。また、実際に取得する場合は、職種によってはそれぞれの職種の団体を通じて取得申請をする場合があります。

日本国内であっても海外の方の個人情報を取り扱う場合は、EU の GDPR (一般データ保護規則) ▶用語集 P.190 など、さらに注意が必要な法制度がありますので、業務を行う前に精査しましょう。

・プライバシーマーク制度 (一般財団法人日本情報経済社会推進協会)

<https://www.jipdec.or.jp/project/pmark.html>

・GDPR (General Data Protection Regulation: 一般データ保護規則) 個人情報保護委員会  
<https://www.ppc.go.jp/enforcement/infoprovision/laws/GDPR/>

と考えて下さい。

P.161で紹介したように、企業のグループ内であっても同様で、問題が発生したときに「関連会社が」とか、「委託先が」といって責任を逃れることは許されません。個人情報を取り扱う者は、会社や団体の社会的な義務を果たし、また、流出した情報に

関してはきちんとした責任を負わなければなりません。

流出がおきれば、実際のお金としての負のコストや、それに対処するためにマンパワー、信用喪失が見えないコストとして、自分たちに跳ね返ってくる点を十分理解して適切な措置を講じる必要があります。



## 付録

# 知っておくと役立つサイバーセキュリティに関する手引き・ガイダンス

本書の最後には、知っておくと役立つ手引きやガイダンスなどを紹介します。サイバー攻撃を受けた場合に相談できる公的機関の窓口、スキルアップしたい中小組織のセキュリティ部門担当者に役立つ情報、そして本格的な普及がはじまったマイナンバーカードなど、実践的な内容を解説します。

また、本章では、「一般国民向け」「中小組織向け」と中心となる対象読者を表すタグを付しています。

**付録01** セキュリティ担当者は知っておきたい「サイバーセキュリティ関係法令Q&Aハンドブック」とは **中小組織向け**

**付録02** サイバー攻撃を受けた場合①～情報関係機関への相談や届け出 **一般国民向け** **中小組織向け**

**付録03** サイバー攻撃を受けた場合②～警察機関への相談や届け出、ガイドライン **中小組織向け**

**付録04** IPAが取り組むさまざまな中小企業向けセキュリティ対策支援 **中小組織向け**

**付録05** IPAのより深いセキュリティ設定資料 **中小組織向け**

**付録06** セキュリティ系業務のアウトソース **中小組織向け**

**付録07** 中小企業がもっとクラウドサービスを利用しやすく！～認定情報処理支援機関(スマート SME サポーター) **中小組織向け**

**付録08** セキュリティの資格取得を目指そう **一般国民向け** **中小組織向け**

**付録09** セキュリティスキルを向上させるには～「CYDER」と「CTF」 **中小組織向け**

**付録10** 本格的な普及がはじまったマイナンバーカード～よくある誤解やセキュリティについて **一般国民向け** **中小組織向け**

## 付録01 セキュリティ担当者は知っておきたい 「サイバーセキュリティ関係法令Q&Aハンドブック」とは

中小組織向け

インターネットが普及した現代、あらゆる事業、ビジネスを進めるにあたって、インターネットやサイバーセキュリティにまつわる法令・法律、それに基づく対応は必須です。一方で、サイバーセキュリティを取り巻く環境は時間の経過とともに変化が激しく、何かしらのトラブルに遭遇した際、時間を要する正規の手続きを経た法律だけでは対応が間に合わないことがよくあります。

加えて、企業が気を付けるべきセキュリティにまつわる関連法令は、本書では取り上げきれないほど範囲が広範のため、企業や組織で情報システムやセキュリティに関する業務の担当者は対応に四苦八苦しているのではないのでしょうか。

こうした中、企業や組織の担当者向けに、内閣官房内閣サイバーセキュリティセンター（NISC）が「サイバーセキュリティ関係法令Q&Aハンドブック」を公開しています。

サイバーセキュリティ関係法令Q&Aハンドブック（令和2年（2020年）3月2日刊行）

[https://security-portal.nisc.go.jp/guidance/pdf/law\\_handbook/law\\_handbook.pdf](https://security-portal.nisc.go.jp/guidance/pdf/law_handbook/law_handbook.pdf)

全体を通じて、次の3つの特徴を持ちます。

①サイバーセキュリティ基本法を筆頭に、サイバーセキュリティに関連すると思われる法令を広範に網羅している

②対象した法令は、ハードローではなくソフトロー（法的な拘束力は

### 企業のセキュリティ部門担当者なら 知っておきたい情報が充実



関係法令 Q & A ハンドブック 配布ページ

[https://security-portal.nisc.go.jp/guidance/law\\_handbook.html](https://security-portal.nisc.go.jp/guidance/law_handbook.html)

ないが事実上、社会的規範として使用されるもの）と呼ばれるガイドラインや技術標準を参考に、可能な限り最新版を参照している

③法令の紹介に加えて、より実際（現場）に即した解説をしていること

この特徴のもと、サイバーセキュリティ対策において参照すべき関係法令を、実例をふまえながら Q&A 形式で解説しています。

例えば、「電子署名、システム開発、クラウド等の契約関連」、「クラウドサービス利活用やモバイル・IoT 機器の活用、それらを含めたテレワークなどの情報通信ネットワーク関連」といった、コロナ禍により普及しよく見かけるようになったシーンに関係する法令から、個人情報保護法や不正競争防止法などサイバーセキュリティだけにとどまらない法律が関係してくる対策事例まで、網羅的に

扱っています。

また、Q&A 方式でサイバーセキュリティ対策やトラブルの対応手順が解説されているため、法律の専門家ではない企業や組織の情報システム部門担当者・セキュリティ担当者でも、実際にトラブルや想定外の出来事に初めて遭遇した際、参考になります。

現場を任されている企業のセキュリティ担当者だけでなく、自社のデータ、情報資産を守る必要のある経営者にも役立つ内容のため、関係者はぜひ一読しておくことをおすすめします。

企業実務として効率的・効果的なサイバーセキュリティ対策・法令遵守を促進することはもちろん、自社・自組織におけるサイバーセキュリティの堅牢性を高めることにつながるでしょう。

## 付録02 サイバー攻撃を受けた場合① ～情報関係機関への相談や届け出

一般国民向け

中小組織向け

P.106-107ではではサイバー攻撃を受けた場合の対処を説明しました。

では会社や団体として、相談したり必要に応じて届け出を行うものとしてはどのようなことを知っておくといのでしょうか。

まず、とりあえずサイバー攻撃を受けたらどこに相談したらいいのか。

代表的なものとしてIPAによる「情報セキュリティ安心相談窓口」があります。同名のウェブサイトを検索すると、「良くある質問」や、過去のサイバーセキュリティに関するレポートなどが掲載されているので、一通り目を通し、それでも解決しない場合は、電話やメールで問合せしてみるとよいでしょう。

「標的型メール攻撃」に関しては「標的型サイバー攻撃特別相談窓口」が個別に設けられています。詳しい情報を提供すると、より速やかに的確な対応ができるようになっていきます。それとは別に、義務ではありませんが、「ウイルスの届け出」「不正アクセスの届け出」を受け付けているので、可能であれば届け出ましょう。そうすることで他の人が攻撃に遭うのを避けることが可能になります。

地域の商工会議所がサイバー攻撃対応支援サービスの一環として、有料の相談窓口を設けている場合もあります。なお業種によって、例えば医療機関でのサイバー攻撃に関しては、厚生労働省が、医政局 研究開発振興課医療技術情報推進室で連絡を受け付けています。また、IPAでは、その年のサイバーセキュリティ上の懸念される脅威を「情報セキュリティ10大脅威」として公開しています。

個人編と組織編に分けて順位付けされており、脅威の内容に加えて、参考事例や注意するポイントがまとまった内容となっています。

さらに、組織を狙った脅威として急激に増えているランサムウェアに関しては、「ランサムウェア対策特

設ページ」が用意されています。万が一、企業や組織でランサムウェアの被害に合った場合、まずこのページをご覧ください、迅速かつ正確な対応を進めていきましょう。

情報セキュリティ10大脅威	
<a href="https://www.ipa.go.jp/security/vuln/10threats.html">https://www.ipa.go.jp/security/vuln/10threats.html</a> ※脆弱性対策 (IPA公開資料一覧ページ) <a href="https://www.ipa.go.jp/security/vuln/index.html">https://www.ipa.go.jp/security/vuln/index.html</a>	
ランサムウェア対策特設ページ	
<a href="https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html">https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html</a>	
IPA情報セキュリティ安心相談窓口	
URL	<a href="https://www.ipa.go.jp/security/anshin/index.html">https://www.ipa.go.jp/security/anshin/index.html</a>
電話での相談	03-5978-7509 (受付時間 10:00～12:00、13:30～17:00、土日祝日・年末年始は除く)
メールでの相談	<a href="mailto:anshin@ipa.go.jp">anshin@ipa.go.jp</a>
FAXでの相談	03-5978-7518
郵送での相談	〒113-6591 東京都文京区本駒込2-28-8 文京グリーンコート センターオフィス 16階 IPAセキュリティセンター 安心相談窓口

### IPA 安心相談窓口で対応出来ない例

なお、IPA 安心相談窓口では、下記のような相談は受け付けていません。

- ・直接来訪しての相談や面談
- ・契約・支払いに関する相談
- ・法的解釈に関する相談
- ・個別の端末調査や犯罪調査に関する相談
- ・特定の製品やサービスの紹介
- ・特定企業への改善や指導に関する相談
- ・パソコンの具体的な操作方法や手順などの案内
- ・他組織への連絡や通報などの仲介

一方、IPA ではなく他の機関が開設している窓口で対応出来る場合もあります。それぞれの窓口の受け付ける事柄を、ウェブサイトなどでよく確認してご相談ください。

#### ●サービス提供または購入などの契約に関するトラブルで困っている場合

消費者ホットライン(消費者庁)  
[http://www.caa.go.jp/region/shohisha\\_hotline.html](http://www.caa.go.jp/region/shohisha_hotline.html)

国民生活センター  
<http://www.kokusen.go.jp/>

#### ●犯罪行為に関する被害届や捜査について相談をしたい場合

都道府県警察本部のサイバー犯罪相談窓口等一覧  
<https://www.npa.go.jp/cyber/soudan.html>

#### ●法的トラブルの相談をしたい場合

法テラス  
<https://www.houterasu.or.jp/>

#### ●インターネット上での違法・有害情報に関し相談したい場合

違法・有害情報相談センター  
<https://www.ihaho.jp/>

社団法人 コンピュータソフトウェア著作権協会  
不正コピー情報受付  
<https://www2.accsjp.or.jp/piracy/>

#### ●インターネット上の違法情報を通報したい場合

インターネット・ホットラインセンター  
<https://www.internethotline.jp/>

#### ●迷惑メールの受信に関して困っている場合

財団法人 日本データ通信協会迷惑メール相談センター  
<https://www.dekyo.or.jp/soudan/ihan/>

#### ●フィッシングサイトの発見または被害に関し困っている場合

フィッシング対策協議会  
<https://www.antiphishing.jp/registration.html>

警察庁 フィッシング110番  
<https://www.npa.go.jp/cyber/policy/phishing/phishing110.htm>

#### ●インターネットに繋がらないなどのトラブルで困っている場合

利用プロバイダまたはパソコンのメーカー・購入店の各サポート窓口

IPA「他の機関が開設している相談窓口等」より  
<https://www.ipa.go.jp/security/anshin/external.html>

## 付録03 サイバー攻撃を受けた場合② ～警察機関への相談や届け出、ガイドライン 中小組織向け

サイバー攻撃では前項のように、自分が攻撃を受けたことに関する相談の他に、実際に情報を盗難されたり、なんらかの被害を被ったり、あるいは法律で禁止されている不正アクセスなどに該当する場合は、警察への相談や通報が必要となります。

まずは都道府県警察本部のサイバー犯罪相談窓口に相談することを最初に考えるとよいでしょう。

その場合でも5W1Hのように「なにがどうなってどういったことが起こっているのか」を、紙に書くなどして整理して明確にし、漠然とした相談にならないようにしましょう。警察がなんらかの捜査をする場合は、そのための情報や証拠が必要となります。

データ損失や不正送金など実害が発生した場合は、やたらにその機器を操作せず、まず相談窓口で相談して対処方針を決めるとよいでしょう。

さてそういった相談窓口を知っておいた上で、大切なのはサイバー攻撃を受けたときにパニックになってどうしてよいかわからなくならないようにすることです。

IPAが公開している「中小企業の情報セキュリティ対策ガイドライン」では、問題が発生したことを想定してシナリオを作っておくことを薦めています。このガイドラインを読むことで、サイバーセキュリティに関するトラブルの発生に「どう備えるか」といことに対するアイデアが得られるので、ぜひ一度目を通して、自分の会社や団体なりの対応マニュアルを作ってみて下さい。

警察庁サイバー犯罪対策プロジェクト	<a href="https://www.npa.go.jp/cyber/">https://www.npa.go.jp/cyber/</a>
各都道府県のサイバー犯罪相談窓口等	<a href="https://www.npa.go.jp/cyber/soudan.html">https://www.npa.go.jp/cyber/soudan.html</a>



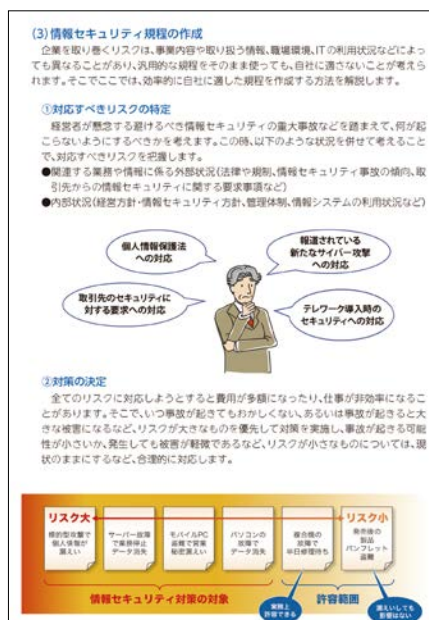
各都道府県警の、サイバー犯罪相談窓口の一覧。

代表の電話番号の場合やサイバー犯罪相談等専用電話番号の場合もあるので、どの電話番号にかけられているのかをよく確認しましょう。

ウェブサイト上のサイバー犯罪に関する情報は、表記されているアドレスだけでなく、他のページにも記載されている場合があります。

### 「中小企業の情報セキュリティ対策ガイドライン」

IPAによる「中小企業の情報セキュリティ対策ガイドライン」は小さな会社やNPOでも役立つ内容が記載されています。ぜひ手に取って役立つ部分を探してみましょう。



<https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html>

情報セキュリティ自社診断シートなどもあるので参考になります。



## 付録O4 IPAが取り組むさまざまな中小企業向けセキュリティ対策支援 中小組織向け

### 1 中小企業の情報セキュリティ対策ガイドラインとは

IPA(独立行政法人情報処理推進機構)は誰もがITの恩恵を享受できるIT社会の実現を目指して、サイバーセキュリティ対策など各種の取り組みを行っている経済産業省所管の政策実施機関です。

そのIPAが発行している「中小企業の情報セキュリティ対策ガイドライン」(以下「対策ガイドライン」)は、ITを何らかの形で経営に活用している中小企業であれば、必ず参照しておくべき指針です。

この対策ガイドラインは、中小企業の経営者に対し、対策の必要性に気づいてもらい、サイバーセキュリティ対策に全く取り組んでいない状態から、徐々にステップアップし、しっかりとした社内ルールと体制を作って組織的なサイバーセキュリティのマネジメント体制を構築する道筋を提供することを目的に編集されています。

ウェブサイトにおいてPDFの電子ファイル版で無償配布されている他、印刷版も有償で提供されています。

この対策ガイドラインの構成は、大きく本編と付録に分かれ、さらに本編は、第1部の「経営者編」と第2部の「実践編」で構成されています。

「経営者編」では、経営者がサイバーセキュリティの必要性を認識し、自らの責任で考え、実行しなければならぬ事項について説明されています。

対策を怠ることで企業が被る不利益や、経営者などが問われる法的な責任、社会的な責任などが、事例や

### 「中小企業の情報セキュリティ対策ガイドライン」とその付録

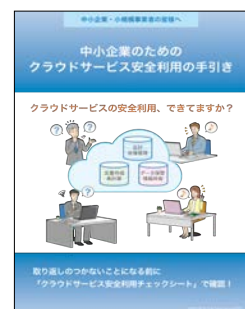
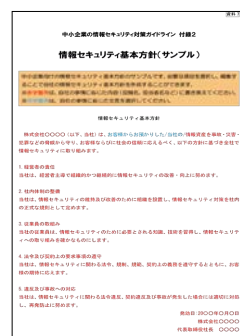
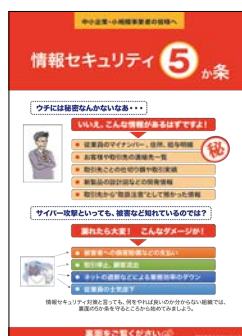


「中小企業のセキュリティ対策ガイドライン」には本編と、各企業が取り組まなければならないチェック項目や、自社のセキュリティ資料を作るためのひな型、そしてクラウドの安全利用のための手続きが含まれます。

中段左から「情報セキュリティ対策5か条チラシ」、中段中「情報セキュリティ基本方針」のサンプル、中段右「5分でできる自社診断」、下段左「情報セキュリティハンドブック」のひな型、下段中「情報セキュリティ関連規程」のサンプル、そして下段右が「中小企業のためのクラウドサービス安全利用の手引き」となっています。

ひな型やサンプルは、文章中の項目を自社の組織や社員名に書き換えればすぐに使えるよう、作られています。

この他にやや専門的になりますが、EXCEL形式の「リスク分析シート」があります。



中小企業の情報セキュリティ対策ガイドライン

<https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html>

主な関係法令の条項と処罰とともに説明されています。そして経営者が認識しておかなければならない「3原則」と、経営者自ら、または、従業員に指示して実行しなければならない「重要7項目の取組」が記述され

ています。

「実践編」では、具体的にどのように対策を進めていくかについて記述されています。

規模の小さな会社や、これまで十分なサイバーセキュリティ対策を実

施してこなかった企業などでも、すぐにできることから開始して、ステップバイステップで、企業それぞれの事情に適した対策が実施できるように、進め方を説明しています。

中でも「情報セキュリティ5か条」は、対策ガイドライン実践編の冒頭で紹介しています。

この5か条は、まず取り組んでいただきたい基本的な対策を最小限にまとめられたものです。ぜひこちらから対策をスタートしてください。

こののち、実践編では、現状を知り改善するステップ、本格的に取り組むステップについて解説しています。

それぞれのステップは、中小企業の実態やサイバーセキュリティ対策のありかたを熟知している有識者により検討された内容となっています。

「付録」は実践編に取り組む際に使用するひな型やシート類です。構成は以下のとおりです。

- 情報セキュリティ対策5か条チラシ
- 情報セキュリティ基本方針(サンプル)
- 5分でできる自社診断
- 情報セキュリティハンドブック(ひな形)
- 情報セキュリティ関連規程(サンプル)
- 中小企業のためのクラウドサービス安全利用の手引き
- リスク分析シート

これらのうち、「5分でできる自社診断」は、25問のチェック項目に回答することで自社の対策状況を把握することが出来るというものです。「基本的対策」、「従業員としての対

## 5分でできる自社診断の25項目

診断項目		No	診断内容	チェック			
				実施している	一部実施している	実施していない	わからない
Part 1 基本的対策	1	パソコンやスマホなど情報機器のOSやソフトウェアは常に最新の状態にしていますか？	4	2	0	-1	
	2	パソコンやスマホなどにはウイルス対策ソフトを導入し、ウイルス定義ファイル※1は最新の状態にしていますか？	4	2	0	-1	
	3	パスワードは破られにくい「長く」「複雑な」パスワードを設定していますか？	4	2	0	-1	
	4	重要情報に対する適切なアクセス制限を行っていますか？	4	2	0	-1	
	5	新たな脅威や攻撃の手口を知り対策を社内共有する仕組みはできていますか？	4	2	0	-1	
Part 2 従業員としての対策	6	電子メールの添付ファイルや本文中のURLリンクを介したウイルス感染に気をつけていますか？	4	2	0	-1	
	7	電子メールやFAXの宛先の送信ミスを防ぐ取り組みを実施していますか？	4	2	0	-1	
	8	重要情報は電子メール本文に書くのではなく、添付するファイルに書いてパスワードなどで保護していますか？	4	2	0	-1	
	9	無線LANを安全に使うために適切な暗号化方式を設定するなどの対策をしていますか？	4	2	0	-1	
	10	インターネットを介したウイルス感染やSNSへの書き込みなどのトラブルへの対策をしていますか？	4	2	0	-1	
	11	パソコンやサーバーのウイルス感染、故障や誤操作による重要情報の消失に備えてバックアップを取得していますか？	4	2	0	-1	
	12	紛失や盗難を防止するため、重要情報が記載された書類や電子媒体は机の上に放置せず、書庫などに安全に保管していますか？	4	2	0	-1	
	13	重要情報が記載された書類や電子媒体を持ち出す時は、盗難や紛失の対策をしていますか？	4	2	0	-1	
	14	離席時にパソコン画面の覗き見や勝手な操作ができないようにしていますか？	4	2	0	-1	
	15	関係者以外の事務所への立ち入りを制限していますか？	4	2	0	-1	
Part 3 組織としての対策	16	退社時にノートパソコンや備品を施錠保管するなど盗難防止対策をしていますか？	4	2	0	-1	
	17	事務所が無人になる時の施錠忘れ対策を実施していますか？	4	2	0	-1	
	18	重要情報が記載された書類や重要なデータが保存された媒体を破棄する時は、復元できないようにしていますか？	4	2	0	-1	
	19	従業員に守秘義務を理解してもらい、業務上知り得た情報を外部に漏らさないなどのルールを守らせていますか？	4	2	0	-1	
	20	従業員にセキュリティに関する教育や注意喚起を行なっていますか？	4	2	0	-1	
	21	個人所有の情報機器を業務で利用する場合のセキュリティ対策を明確にしていますか？	4	2	0	-1	
	22	重要情報の授受を伴う取引先との契約書には、秘密保持条項を規定していますか？	4	2	0	-1	
	23	クラウドサービスやウェブサイトの運用等で利用する外部サービスは、安全・信頼性を把握して選定していますか？	4	2	0	-1	
	24	セキュリティ事故が発生した場合に備え、緊急時の体制整備や対応手順を作成するなど準備をしていますか？	4	2	0	-1	
	25	情報セキュリティ対策(上記1～24など)をルール化し、従業員に明示していますか？	4	2	0	-1	

※1 コンピュータウイルスを検出するためのデータベースファイル「パターンファイル」とも呼ばれる  
 ※2 重要情報とは営業秘密など事業に必要で組織にとって価値のある情報や顧客や従業員の個人情報など管理責任を伴う情報のことです

**診断の後は次ページ以降を読んで対策を検討してください。**

A 実施している 合計点	B 一部実施している 合計点	C わからない 合計点	
点	点	点	点
<b>A+B+C 合計</b>			点

付録「5分でできる自社診断」の中にある、診断のための25項目。それぞれの項目に答えることで自社のセキュリティレベルが診断できます。

先々どういったセキュリティ項目を満たしていけないといけないか、というビジョンを持つためには目を通しておくとういでしょう。

情報セキュリティ対策支援サイトでもオンラインで診断ができます。

<https://security-shien.ipa.go.jp/learning/>



策」及び「組織としての対策」という構成になっており、「基本的対策」は前述の「情報セキュリティ5か条」と同じになっています。

これに加え、「従業員としての対

策」では、電子メール利用時や情報を格納した機器などの持ち出し、管理、バックアップなどの13項目、「組織としての対策」では、従業員教育や、取引先との契約時の秘密保持、

緊急時の体制整備、ルール化など7項目が設けられています。これら25項目により、サイバーセキュリティ対策の実施状況を点数化し100点満点でどの程度の達成状況か、また、どのような項目が弱点かを測ることができ、対策に取り組むうえでのポイントを見える化することが出来ます。

同じく、付録に収められている「情報セキュリティ基本方針」や「情報セキュリティ関連規程」のサンプルは、それぞれ、自社の状況や方針に沿って記述を選択、あるいは書き換えることで自社固有のものに上げることが可能です。また、「情報セキュリティハンドブック」(ひな型)は、社内ルールに合わせて書き換えができますので、従業員ひとりひとりへのルール徹底に役立ちます。

## 2 サイバーセキュリティ対策自己宣言「SECURITY ACTION」

「SECURITY ACTION(セキュリティアクション)」制度は、中小企業がサイバーセキュリティ対策に自発的に取り組むことを社の内外に宣言する制度です。

IPAの他、商工団体、中小企業に関係する土業団体などが連携して創設し、IPAが運用を行っています。

サイバーセキュリティ対策を始めたくても「なにをすればよいかかわからない」、「経営者が重要性を認識してくれない」という中小企業の実態(IPAが実施した実態調査より)を踏まえ、まず何をすべきか、よりよくするために何をすべきか、ということを示し、実際に取り組んでいることを中小企業に自己宣言してもらおう、というのがこの制度の趣旨です。

SECURITY ACTION は、現在「一つ

## 情報セキュリティ関連規程のサンプル

1	組織的対策	改訂日	20yy.mm.dd
適用範囲	全社・全従業員		

1. 情報セキュリティのための組織

情報セキュリティ対策活動を推進するための組織として、**情報セキュリティ委員会**を設置する。

**情報セキュリティ委員会**は以下の構成とし、情報セキュリティ対策状況の把握、情報セキュリティ対策に関する指針の策定・見直し、情報セキュリティ対策に関する情報の共有を実施する。

情報セキュリティ委員会	
情報セキュリティ責任者	代表取締役
情報セキュリティ 部門責任者	各部長
システム管理者	総務部長
教育責任者	人事部長
インシデント対応責任者	〇〇〇〇部長
個人情報 苦情対応責任者	
監査・点検/点検 責任者	〇〇〇〇課長
特定個人情報 事務取扱責任者	代表取締役
特定個人情報 事務取扱担当者	総務部長

体制図を下図に示す。組織の変更があった場合は、**情報セキュリティ責任者**が本体制図の更新を行う。

最高  
情報セキュリティ  
責任者  
代表取締役

システム管理者

教育責任者

・インシデント  
対応責任者  
・個人情報  
苦情対応責任者

特定個人情報  
事務取扱責任者

特定個人情報  
事務取扱担当者

監査・点検  
責任者

情報セキュリティ  
部門責任者  
〇〇部長  
△△部長  
□□部長

付録「情報セキュリティ関連規程」のサンプルの中の「組織内対策」のページ。

用意されたサンプルの中の赤字の部分を自社の情報に書き換えていくことで、自社の「情報セキュリティ関連規程」が完成するようになっています。

関連規程といってもなにを盛り込んでよいかわからないといったことが、このサンプルをなぞることで解決されます。

## ウェブサイトに掲載するSECURITY ACTIONのマーク



SECURITY ACTION の条件を満たした上で、これらのマークをウェブサイトに掲載することで、外部の企業などに対して自社のサイバーセキュリティに対する取り組みの「本気度」を示すことができます。

星」と「二つ星」の2段階があります。一つ星は「情報セキュリティ対策5か条」に取り組むことを宣言するもの、二つ星は、「5分でできる自社診断」で自社の状況を把握するとともにサイバーセキュリティ基本方針を定めてウェブサイト上などで外部に示したことを宣言するものです。これらは、「中小企業向け情報セキュリティ対策ガイドライン」と同調していま

す。  
この宣言をすることにより、社内意識の醸成、また、社外からは取り組みを評価され、信頼の獲得と向上につながるなどの効果が期待できます。  
まずは始める、その一歩としてSECURITY ACTION を宣言してはいかがでしょうか？

(執筆：IPA)



### 3 サイバーセキュリティお助け隊サービス

前述したガイドライン、「SECURITY ACTION」の内容を読めばセキュリティ対策の知識を深めることはできますが、実際にサイバー攻撃を防ぐための対策を講じると、費用面でも時間面でもコストがかかります。

人材・体制・資金などのリソースが限られている多くの中小企業にとって、通常業務をこなしながらセキュリティ対策を講じるための負担は少なくありません。

そんな中小企業の負担を軽減するためにも、IPAでは「サイバーセキュリティお助け隊サービス」を2021年度から運用しています。

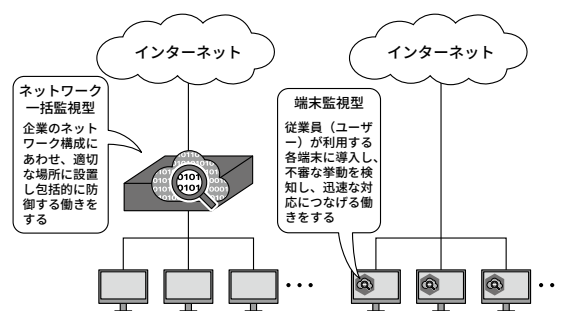
IPAは2019年度、2020年度の時点から、中小企業への攻撃実態把握や中小企業向けのサイバーセキュリティ対策支援のしくみを構築するため、「サイバーセキュリティお助け隊実証事業」を実施し、この事業で得られた知見をもとに中小企業にとって不可欠なセキュリティサービスを示す「サイバーセキュリティお助け隊サービス基準」を制定しました。そしてこのサービス基準を充足する民間サービスには「サイバーセキュリティお助け隊マーク」を付与し普及を促進することで、多くの中小企業へ無理なくサイバーセキュリティ対策を導入・運用することを支援しています。

2023年1月時点で、「サイバーセキュリティお助け隊サービス」ではサービス基準を満たす20以上のセキュリティサービスが提供されています。

サービスの具体的内容は、

- ・中小企業のサイバーセキュリティ対策を支援するための相談

### 「サイバーセキュリティお助け隊サービス」における異常監視のしくみ

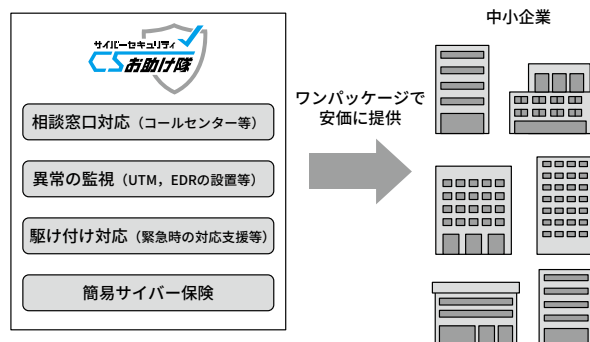


セキュリティ対策では、目に見えないサイバー攻撃を可視化し、侵入などの異常に早く気付くことがもっとも大切です。サイバーセキュリティお助け隊サービスでは、ネットワーク一括監視型、端末監視型、またはその両方（併用型）による異常の監視を提供しています。

### 「サイバーセキュリティお助け隊サービス」案内ページ

ユーザー向けサイト	<a href="https://www.ipa.go.jp/security/otasuketai-pr/">https://www.ipa.go.jp/security/otasuketai-pr/</a>
IPA案内ページ	<a href="https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html">https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html</a>
概要説明資料(PDF)	<a href="https://www.ipa.go.jp/files/000100463.pdf">https://www.ipa.go.jp/files/000100463.pdf</a>

### 「サイバーセキュリティお助け隊サービス」で提供するサービス内容



中小企業がサイバー攻撃への対処として不可欠なサービスを効果的、網羅的にカバーし、かつ安価に提供しています。

窓口

- ・UTM（Unified Threat Management・統合脅威管理）などのネットワークセキュリティ監視装置を用いたユーザーのネットワーク通信の異常を一括監視、またはEDR（Endpoint Detection and Response）などエンドポイントセキュリティソフトウェアを用いたユーザーの端末の異常を監視（両方が提供されるサービスもあり）
- ・サイバー攻撃発生時の初動対応

（駆け付け支援など）

- ・被害に遭った際に備える簡易サイバー保険

などがあり、中小企業がサイバー攻撃への対処として不可欠なサービスを効果的、網羅的にカバーし、かつ安価に提供しています。

企業経営において省くことはできないセキュリティ対策に悩んでいる中小企業にとって、効果的なセキュリティサービスをワンパッケージで利用できるようになっています。



## 付録05 IPAのより深いセキュリティ設定資料

中小組織向け

ITの特徴は、多くの人の目的に合致するように柔軟に作られていることで、機器であれソフトであれ多くの設定項目が用意されており、それを調整することでより自分の目的に適した使い方が可能になります。基本的には標準設定のままで十分使えるようになっていますが、まずはそのままで生産性を上げることを目指すのが大事です。しかし、将来的にもっとセキュリティ性を高めて安全に使いたいと思う時期がやってきます。

そうしたときにはIPA(独立行政法人情報処理推進機構)のウェブサイ

トに紹介されているマニュアルなどが参考になります。「情報漏えいを防ぐためのモバイルデバイス等各種設定マニュアル」では、一般従業員層にもできれば最低限知っておいてほしい暗号化の必要性や仕組み、情報漏えい対策として機能させるために必要なことなどを、平易な表現でまとめています。「TLS暗号設定ガイドライン」ではウェブサイトを作成し公開するときに、適切な暗号化通信の運用について解説しています。

「IT製品の調達におけるセキュリティ要件リスト活用ガイドブック」

では、経済産業省が公開している「IT製品の調達におけるセキュリティ要件リスト」に対し、これを実際にどのように活用するか辞書的な役割を担うものです。

「IT製品の調達におけるセキュリティ要件リスト」は「国際標準ISO/IEC 15408に基づくセキュリティ要件」に適合することが認証されたセキュリティ製品のリストで、それをどう活用するかが解説されています。

いずれも、本書に書かれているセキュリティ知識を習得した上で、次のステップに進む手引きとなる資料です。

### 情報漏えいを防ぐためのモバイルデバイス等各種設定マニュアル

[https://www.ipa.go.jp/security/ipg/documents/dev\\_setting\\_crypt.html](https://www.ipa.go.jp/security/ipg/documents/dev_setting_crypt.html)

### TLS暗号設定ガイドライン～安全なウェブサイトのために(暗号設定対策編)～

[https://www.ipa.go.jp/security/vuln/ssl\\_crypt\\_config.html](https://www.ipa.go.jp/security/vuln/ssl_crypt_config.html)

### IT製品の調達におけるセキュリティ要件リスト活用ガイドブック

<https://www.ipa.go.jp/security/it-product/guidebook.html>

## 付録06 セキュリティ系業務のアウトソース

中小組織向け

小さな会社やNPOのみなさんがより責任ある立場になっていくためには、本格的にサイバーセキュリティに取り組む必要があります。ただし、小さな会社やNPOにとって、それらを自ら習得するのは困難です。そういった状況で、インターネットの特性を生かし、専門の企業にアウトソースすることで、堅牢性を担保するのも1つの手でしょう。

しかし、みなさんにとっては「どいういった企業が信頼できるのか」というところからのスタートになると思いますので、そういったシーンに向けて、経済産業省とIPAでは「情報セキュリティサービス基準適合サービスリスト」を公開しています。つまり、一定の基準を満たしたセキュリティ系企業のリストを公開しています。

リスクアセスメントを行う「情報セキュリティ監査」、ウェブサイトやシステムの弱点を見つける「脆弱性診断」、被害に遭ったときの鑑識的業務を行う「デジタルフォレンジック」、そして日々の問題無く業務行えるか常にチェックをする「セキュリティ監視・運用」の、それぞれのリストがあります。

### 情報セキュリティサービス基準適合サービスリスト(IPA)

[https://www.ipa.go.jp/security/it-service/service\\_list.html](https://www.ipa.go.jp/security/it-service/service_list.html)

### 情報セキュリティサービス審査登録制度(経済産業省)

<http://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html>

### 情報セキュリティサービス基準(経済産業省)

<http://www.meti.go.jp/policy/netsecurity/shinsatouroku/zyouhoukizyun.pdf>

## 付録07 中小企業がもっとクラウドサービスを利用しやすく！ ～認定情報処理支援機関(スマート SME サポーター)～

中小組織向け

認定情報処理支援機関(スマート SME サポーター)とは、経済産業省の外局である中小企業庁が運営する、中小企業のIT活用を支援するITベンダーなどを中小企業等経営強化法に基づいて「情報処理支援機関」として認定する制度です。

近年、IT技術の進展や通信回線の高速化によって、サーバーなどの設備を持たなくてもソフトウェアの利用が可能なクラウドサービスの提供が増えてきました。

クラウドサービスは、設備やソフトウェアを購入する必要が無いため、初期導入コストが低く、しかも経営指導の専門家などとも情報共有がしやすく、クラウドサービス同士を組み合わせて活用することができるなど、中小企業にとっても数々のメリットがあります。

一方で、セキュリティ実装状況や保存したデータの取扱い条件などに関する情報提供が、クラウドサービスを提供するITベンダーによって異なり、中小企業にとっては分かりにくい部分がありました。

中小企業庁では、専門家との検討により、①クラウドサービスの安全・信頼性に関する情報、②セキュリティ対策状況、③利用者のサポート体制、④利用終了時のデータの取扱い、などの確認すべき項目を定めて、スマート SME サポーターの認定申請時にITベンダーから申告させ、認定後には中小企業庁が特設サイトにて公開しています。

上記の項目の詳しい確認方法については、IPAが「中小企業のためのクラウドサービス安全利用

### 情報処理支援機関検索

情報処理支援機関として認定された、みなさんの生産性を高める IT ツールを提供する IT ベンダーが検索出来ます。

本書ではコンテンツを作る業種を例に挙げましたが、この検索を用いることで、業種別、サービス別、そして地域別に、必要としているベンダーの情報を得ることが出来ます。

例えば、「東京都」で「飲食・サービス」業で、「予約」システムを提供してくれる会社を知りたい、というように検索します。

の手引き(<https://www.ipa.go.jp/files/000072150.pdf>)」で解説していますので、参照下さい。

その他、同じく IPA が提供する「中小企業の情報セキュリティ対策ガイドライン(<https://www.ipa.go.jp/security/keihatsu/sme/guideline/>)」、「SECURITY ACTION セキュリティ対策自己宣言」(<https://www.ipa.go.jp/security/security-action/>)や経済産業省が提供する「中小企業のサイバーセキュリティ対策」(<https://www.meti.go.jp/policy/netsecurity/sme-guide.html>)」も参考になります。

便利な IT ツールでも、利用者がデータを取り出せなかったり、セキュリティ対策がおろそかでは、安心して使い続けることができません。

スマート SME サポーターとして公開されている情報を参考にして、クラウドサービスなどの中小企業にとって生産性向上に役立ち安全・安心に使える IT ツールを上手に選んで活用しましょう。

### ● Smart SME Supporter 情報処理支援機関検索

<https://smartsme.secure.force.com/smartsmesearch/>

## 付録08 セキュリティの資格取得を目指そう

一般国民向け

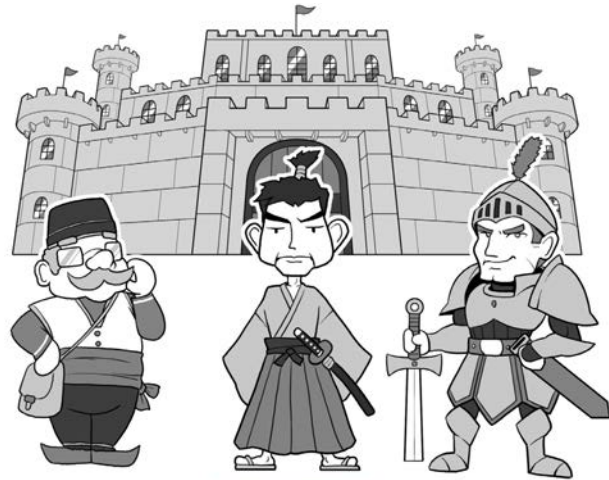
中小組織向け

セキュリティについて深く知りたい、もっと詳しく学びたいと考えているのであれば、オススメしたいのが資格の取得を目指した勉強です。すでにセキュリティ関連の資格は数多く存在していて、自分自身のレベルや目的に合わせて選択できる環境が整っている他、資格取得のための勉強を進めることで、体系立てて知識を獲得できるメリットがあります。

そうしたセキュリティ関連の資格として、比較的取り組みやすいものの1つに「情報セキュリティマネジメント試験(セキユマネ)」があります。これは、脅威から継続的に組織を守るための基本的なスキルを認定する試験であり、業務で個人情報を取り扱ったり、情報管理を担当したりするすべての人を対象としています。サイバーセキュリティについて、基礎知識からバランスよく学習したいと考えているのであれば、まずはここからチャレンジするのも1つの方法です。

さらに、高度な資格としては、「情報処理安全確保支援士」やグローバルで普及している「CISSP」(Certified Information Systems Security Professional)などがあります。情報処理安全確保支援士はサイバーセキュリティに関する実践的な知識や技能を有する専門人材の育成や確保を目的とした国家資格制度であり、サイバーセキュリティに関する高度な知識と技能を持つことを証明することができます。一方、CISSPは(ISC)2(International Information Systems Security Certification Consortium)が認定を行う、国際的なサイバーセキュリティのプロ

### 数多くあるセキュリティ資格



セキユマネ

情報処理安全  
確保支援士

CISSP

現在、セキュリティに関する資格試験は数多くあり、自分のレベルや目的に合わせて取得することが可能です。サイバーセキュリティに特化した試験にチャレンジする前に、ITに関する全般的な知識が問われる「ITパスポート試験」を受けてみるのもよいでしょう。そして、情報処理安全確保支援士の「士」は騎士や武士の「士」。現代の騎士や武士としてセキュリティを守りましょう。

### セキュリティを網羅的に学ぶことができる



資格取得を目指して勉強する大きなメリットは、その領域に関する知識を段階的かつ網羅的に学べることにあります。また、自分の知識レベルを判断する上でも、こうした試験は大いに役立ちます。

フェッショナル認証資格です。これらの資格取得に向けた勉強を積み重

ねれば、自身のスキルアップにもつながるでしょう。

ブ  
ロ  
ー  
グ

第  
1  
章

第  
2  
章

第  
3  
章

第  
4  
章

第  
5  
章

第  
6  
章

第  
7  
章

付  
録



専任のセキュリティ担当者がいない中小企業やNPOなどの場合、サイバー攻撃から身を守る手段は、主として「攻撃を受けにくくなる」ようにすることや、自社のウェブサイトを持つ場合でも、ホスティングサービスを利用することで、セキュリティに割く労力をアウトソースすることといった対応が現実的です。

しかし、サイバー攻撃に対して「立ち向かう」ことが求められる状況も出てきます。では実際にどうやって立ち向かえばよいのでしょうか。

## ●CYDER

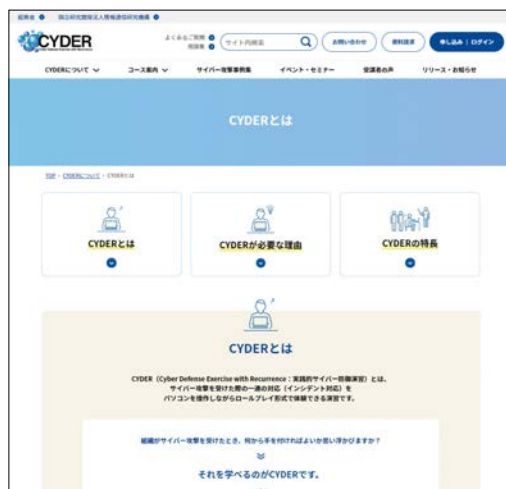
そこで参考にしたい取組が、国立研究開発法人情報通信研究機構(NICT)が国・地方公共団体・独法・重要インフラ事業者などの情報システム担当者などを対象に提供している実践的サイバー防御演習「CYDER(CYber Defense Exercise with Recurrence)」です。

CYDERの受講者は、事前オンライン学習によって攻撃手法や対策技術に対する理解を深め、集合演習(ハンズオン&グループワーク)を通じて、一連のインシデントハンドリングを体験することにより、組織で役立つセキュリティポリシーやコミュニケーションの重要性を学ぶことができます。

とくに小さな組織では、情報システム担当者を専任で配置することが困難な場合があります。しかし、サイバー空間では、組織の規模に関係なく、攻撃されるリスクにさらされています。

経営者1人で対策を考えるのではなく、CYDERのようにコンパクト

## 実践的サイバー防衛演習「CYDER」



CYDERのウェブサイトではCYDERのリーフレットや、その実習内容を紹介するPDFなどが公開されています。

左図のように仮想空間上に現実のネットワークに似たネットワークを構築して、サイバー攻撃への対処方法を実践的に体得できます。

2022年12月現在、CYDERにはレベルに応じたA～Cコース、およびオンラインコースが用意されています。とくに初級レベルのAコースは全国47都道府県で開催されますので、国・地方公共団体・独法・重要インフラ事業者などの情報システム担当者などでご興味のある方は参加をおすすめします。

実践的サイバー防御演習「CYDER」	<a href="https://cyder.nict.go.jp/">https://cyder.nict.go.jp/</a>
セキュリティ国際会議「DEFCON」	<a href="https://defcon.org/">https://defcon.org/</a>
特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)SECCON実行委員会主催「SECCON」2022	<a href="https://www.seccon.jp/2022/">https://www.seccon.jp/2022/</a>

にまとまった訓練の機会を積極的に利用するとよいでしょう。組織のサイバー攻撃対応力をつけることが、有事に備えることにつながるのです。

## ●CTF

体系的な訓練以外に、さまざまな団体がコンテスト形式で行うサイバーセキュリティコンテストも存在します。それがCTF(Capture The Flag)です。

参加者は自身の知識や技術を活用

して隠された答え(Flag)を見つけ出し、時間内に獲得した合計点数を競います。その他、ネットワーク内で擬似的なサイバー空間での攻防を行い競い合う形式のものもあります。

有名なものでは、アメリカで毎年夏に開催される世界最大のセキュリティ国際会議DEFCONが主催するCTF、また、日本国内では特定非営利活動法人日本ネットワークセキュリティ協会(JNSA)SECCON実行委員会が主催するSECCONが有名です。



## 付録10

# 本格的な普及がはじまったマイナンバーカード ～よくある誤解やセキュリティについて

一般国民向け

中小組織向け

## 代表的なマイナンバーカードによるメリット



メリットいっぱい! マイナンバーカード | デジタル庁

[https://www.digital.go.jp/assets/contents/node/basic\\_page/field\\_ref\\_resources/68bc86d6-94d7-4fe8-a592-302d78828e1f/f1c7e648/20221003\\_policies\\_mynumber\\_pros-and-safety\\_leaflet\\_01.pdf](https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/68bc86d6-94d7-4fe8-a592-302d78828e1f/f1c7e648/20221003_policies_mynumber_pros-and-safety_leaflet_01.pdf)

私たちの生活に深く関わる行政サービスの中で、ここ2,3年で大きな動きがあったものの1つとしては、マイナンバーカードの普及があります。総務省がマイナンバーカード交付状況を公開していますが、2022年10月時点でついに全国の交付状況が50%を超え、国民の半数以上がマイナンバーカードを所持するようになり、着実に普及率は高まっています。

マイナンバーカード交付状況について | 総務省  
[https://www.soumu.go.jp/kojinban\\_go\\_card/kofujokyo.html](https://www.soumu.go.jp/kojinban_go_card/kofujokyo.html)

令和6年(2024年)秋ごろには、マイナンバーカードと健康保険証を一体化し紙の健康保険証を廃止するなど今後も活用の幅が広がられていくことが予定されています。

このマイナンバーカードを活用するにあたって、国民1人ひとり、セキュリティ上どのようなリスクがあり、どんなことを意識すべきなのでしょう。

日本政府、省庁、さまざまな関係機関がマイナンバーを普及させるために、多くのガイダンスや手引きを公開しています。公開されている情報を参考に、マイナンバーカード、マイナンバー制度を安全に利活用す

るために必要な知識を把握しましょう。

## ●マイナンバー、マイナンバーカード導入の目的とは?

そもそも、マイナンバーカードを普及させるマイナンバー制度とは、どのような目的で導入されたのでしょうか。マイナンバー制度の概要については、総務省、デジタル庁が公開している情報に詳細な説明があります。

マイナンバー制度 | 総務省  
[https://www.soumu.go.jp/kojinban\\_go\\_card/01.html](https://www.soumu.go.jp/kojinban_go_card/01.html)

ブ  
ロ  
ー  
グ

第  
1  
章

第  
2  
章

第  
3  
章

第  
4  
章

第  
5  
章

第  
6  
章

第  
7  
章

付  
録

## 誤解されがちなマイナンバーカードの安全性について

**知って安心！**  
**マイナンバーカードの使い方**

**持ち歩き方**  
 普通に持ち歩いていいの？  
 ええんじやよ。キャッシュカードの感覚が近いの。失くさないようにするのじゃよ！

**提示方法**  
 銀行や勤務先などでマイナンバーの提示を求められたときはどうすればいい？  
 おもて・うら両面を見せるのじゃ。  
 じゃあレンタルショップなどで、本人確認書類として使うときは？  
 おもて面を見せるのじゃ。その際、うら面のマイナンバーは見られても大丈夫じゃが、マイナンバーを書き留めたりコピーを取るとはダメなのじゃ。

**暗証番号**  
 暗証番号を友達に教えても大丈夫？  
 キャッシュカードと同様、他人に教えてはいけないのじゃ。暗証番号はマイナンバーカードを利用するために必要な大事なもののじゃよ！

**SNSヘカードの画像の投稿は??**  
 こんなに安全なら、カードを自慢しても大丈夫？  
 マイナンバーを誰かに知られても大丈夫なように安全対策は施されているが、不特定多数の目に入る場所への投稿は禁止されているのじゃ！

**まとめ！**  
**マイナンバーカードは安全です！**

**なりすましはできません**  
 顔写真入りのため、対面での悪用は困難。  
**マイナンバーを見られても悪用は困難**  
 マイナンバーを利用するには、顔写真付き本人確認書類などで本人確認をする必要があるため、悪用は困難。  
**プライバシー性の高い個人情報が入っていません**  
 オンラインの利用には電子証明書を使うため、マイナンバーが使われることはありません。  
 ICチップ部分には、税や年金などの個人情報は記録されません。  
**プライバシー性の高い対策**  
 紛失・盗難の場合は、24時間365日体制で一時的利用停止可能  
 アプリ毎に暗証番号を設定し、一定回数間違えると機能ロック  
 不正に情報を読み出そうとすると、ICチップが壊れる仕組み

**マイナンバーについてのお問合せ**  
**マイナンバー総合フリーダイヤル**  
**0120-95-0178**  
 平日：9時30分～20時00分 土日祝：9時30分～17時30分（年末年始を除く）  
 転失・盗難によるマイナンバーカードの一時利用停止については24時間365日受付  
 ■一部のIP電話等で上記ダイヤルに繋がらない場合  
 マイナンバーカード 総合お問合せ  
**050-3818-1250 050-3816-9405**  
 ■英語、中国語、韓国語、スペイン語、ポルトガル語対応のフリーダイヤル  
 This telephone number is toll-free corresponding to English, Chinese, Korean, Spanish and Portuguese.  
 Inquiries about Social Security Inquiries about Notification Card and Tax Number System  
**0120-0178-26 0120-0178-27**  
 https://www.kojinbango-card.go.jp/forhelpdesk

**安全性**  
**マイナンバーカードの**  
**安全性**  
 教えて!!  
 マイナンはあちゃん  
 マイナンバー  
 プリキヤワクター  
 マイナン  
 万全なのじゃ  
 マイナンバーの生き字引  
 マイナンはあちゃん  
 デジタル庁 総務省

マイナンバーカードは顔写真入りのため、対面ではなりすましの悪用は困難です。また、利用時にはあわせて本人確認をする必要があるため、マイナンバーそのものを見られてもすぐに何かに悪用されることは難しく、マイナンバーカードやICチップには税や年金などの個人情報は記録されていません。

アプリ毎に暗証番号を設定し、一定回数間違えるとロックがかかり、不正に情報を読み出そうとすると、ICチップが壊れる仕組みも採用されています。

詳細な説明はデジタル庁のウェブサイトにもあります。

マイナンバー（個人番号）制度 | デジタル庁

<https://www.digital.go.jp/policies/mynumber/>

上記公開情報にある説明を簡単にまとめると、マイナンバー制度導入のおもな目的は、複数の行政機関の間で連携・確認を必要としていた行政手続きの簡略化・簡便化です。

これまで、社会保障・税関係の行政手続きには、国民自らが市区町村役場、税務署など複数の行政機関に照会して書類を都度入手し、提出する、といった面倒な手間をかける必要がありました。

しかしマイナンバー制度を導入することで、複数の行政機関がバラバ

らに保有する個人の情報を同一人物の情報であることの特典・連携がスムーズになり、行政手続きの簡略化・簡便化を図ることができます。

そして、マイナンバーカードには、カード裏面とカードに搭載されたICチップにマイナンバーが記載されています。

このマイナンバーカードを活用することで、「マイナンバーカードを利用する」「コンビニで社会保障・税関係の各種証明書を取得する」「マイナポータルを利用する」「民間のサービスとも連携する」など、従来は複数の行政機関にまたがり手続きが必要だったサービスを簡単に受けられるようになり、国民生活の利便

性向上が見込まれています。

### ●マイナンバー制度、よくある誤解

マイナンバーは12桁の番号で、平成27年(2015年)10月に施行された「行政手続における特定の個人を識別するための番号の利用等に関する法律」(通称：マイナンバー法)という法律により、国民1人ひとりに、すでに固有の番号が割り当てられています。

よくある誤解としては、「政府がマイナンバーを使用して国民の個人情報を一元管理、監視しているのでは?」といったものを見聞きしますが、マイナンバー法の施行で行われたことは国民1人ひとりへの番号割り当てであって、その番号に紐づく

## 紛失した場合の相談窓口は24時間365日対応

The screenshot shows the 'マイナンバーカード総合サイト' (My Number Card Comprehensive Site). The main navigation bar includes links for '申請・受取方法 申請状況確認', '紛失・一時停止 セキュリティ', 'よくあるご質問', 'マイナンバー (個人番号) とは', 'マイナンバーカード について', and '交付申請書等 ダウンロード'. The page title is 'お電話でのお問い合わせ' (Contact by phone). A red banner states: '間違い電話が増えています。お掛け間違いのないよう十分に注意してください。' (There is an increase in wrong calls. Please be very careful not to make wrong calls). Below this, it says 'マイナンバーに関するお問い合わせ' (Contact regarding My Number) and 'マイナンバー総合フリーダイヤル' (My Number Comprehensive Free Dial). The phone number '0120-95-0178' is displayed with a phone icon. There is a chat button 'チャットで 質問する' and a button 'オンライン申請はこちら' (Online application here).

お電話でのお問い合わせ | マイナンバーカード総合サイト  
<https://www.kojinbango-card.go.jp/contact/tel/>  
 マイナンバー総合フリーダイヤル：0120-95-0178

さまざまな個人情報(保険証、住民票、パスポートなど)は、複数の行政機関(各省庁や自治体)が別々に(年金の情報は年金事務所、地方税の情報は市区町村といったように)管理しています。

そして、法律に規定があるものを除いて、マイナンバーをその内容に含む個人情報の利用、提供、収集などする行為は、マイナンバー法(第15条(提供の求めの制限)、第19条(特定個人情報の提供の制限)、第20条(収集等の制限)など)でも明確に禁止されています。

行政手続における特定の個人を識別するための番号の利用等に関する法律施行令

<https://elaws.e-gov.go.jp/document?lawid=426CO0000000155>

マイナンバーは、複数の機関に存

在する特定の個人の情報を同一人の情報であるということの確認を行うために使用されます。

そして不正な利用が行われないように、監査権限を有した第三者機関である「個人情報保護委員会」が監視・監督しています。

しかし、前述した誤解は「自分の個人情報を知らない内に管理されるのは怖い」といった不安や懸念から生じているのであり、センシティブな個人情報の取り扱いにおいて、そのような不安を多かれ少なかれ感じることが健全な感覚、セキュリティ意識といえるでしょう。

そこで政府としても、マイナンバー制度に対する不安を払拭し、国民からの理解を得られるように、マイナンバー、マイナンバーカードの安全性周知には力を入れています。

マイナンバーカードのメリットと安

全性 | デジタル庁

<https://www.digital.go.jp/policies/mynumber/pros-and-safety/>

### ●マイナンバーカード利用時の注意とは

それでは、私たち国民一人ひとりがマイナンバーを利用する際、セキュリティ上、どんなことを意識すべきなののでしょうか？

まず大事なことは、マイナンバーカードを紛失しないこと、そして紛失した場合は即時停止措置を講じることです。

紛失した際に利用を即時停止できる24時間365日対応可能な電話窓口も用意されています。

カード紛失に気付いた場合はすぐに、以下電話番号までカードの一時停止を申し込み、カードの第三者によるなりすまし利用を防止しましょう。



次に気を付けたいことは、暗証番号の管理です。

暗証番号は、銀行のキャッシュカードなどと同じで、むやみに誰かに伝えてはいけません。忘れないように、そして盗み見られたりしないように管理しましょう。

マイナンバーカードに設定できる暗証番号は、①署名用電子証明書用、②利用者証明用電子証明書用、③住民基本台帳用、④券面事項入力補助用の4つで、①は6文字以上16文字以下の英大文字と数字で、②,③,④は数字4桁です。

暗証番号を忘れた場合、再設定も可能ですが、自治体の窓口へ直接問い合わせしなければならず手間がかかります。マイナンバーカードを発行する際、自治体によっては暗証番号の紛失に備えて暗証番号を記録するシートやメモなどをあわせて渡されますが、しっかりと自分だけが確認できる状態で安全に保管しましょう。具体的には、P.120「コラム.2 パスワードの管理と流出チェックについて」、P.122「コラム.3 パスワードを記録する演習」に、パスワードを紙で管理する場合の安全管理方法を解説しているので、参考にしてください。

### ●企業がマイナンバーの管理運用で気を付けるべきことは

企業が従業員のマイナンバーの取り扱いに気を付ける際には、個人情報保護委員会が公開している「特定個人情報の適正な取扱いに関するガイドライン」が参考になります。

特定個人情報の適正な取扱いに関するガイドライン | 個人情報保護委員会

<https://www.ppc.go.jp/legal/policy/>

## 個人情報保護委員会が公開している企業向けのマイナンバー管理運用に関するハンドブック

### やさしい マイナンバー(個人番号) ハンドブック

～ マイナンバー(個人番号)の  
基本的な理解のために ～



平成31年3月

PPC 個人情報保護委員会

やさしいマイナンバー(個人番号)ハンドブック～マイナンバー(個人番号)の基本的な理解のために～ | 個人情報保護委員会

[https://www.ppc.go.jp/files/pdf/yasashii\\_handbook.pdf](https://www.ppc.go.jp/files/pdf/yasashii_handbook.pdf)

とくに、上記ガイドラインの「特定個人情報に関する安全管理措置」では、「安全管理措置の検討手順」「講ずべき安全管理措置の内容」といった記載があり、企業がマイナンバーを適切に管理するための手順がまとめられています。

安全管理措置には、「組織的安全管理措置」「人的安全管理措置」「物理的安全管理措置」「技術的安全管理措置」の4つが定められていて、

情報漏えいなどのリスク対策といった具体的な方法が説明されているので、企業のセキュリティ担当者の方はチェックするとよいでしょう。

ただ、上記のガイドラインは長文で読み解くには時間もかかるため、マイナンバーの概要をやさしく解説した「やさしいマイナンバー(個人番号)ハンドブック」も公開されています。忙しい人はまずはこちらから確認してみてください。



## おわりに～インターネットとよい付き合いを続けるために

今や、誰もがパソコンやスマホを持ってインターネットにつながるものが当たり前になり、民間企業・公的機関問わず、無料・有料含めて、多くの便利なサービスを利用できる時代になっています。

とくにスマホの普及は、多くの人の生活を激変させ、今後もまだまだ新しいサービスが出てきています。便利があふれる一方で、インターネット上で悪いことを考える人たちも増えており、サイバー攻撃による被害は多くなっています。

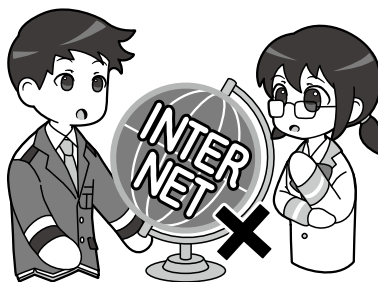
本書で説明した、サイバーセキュリティの考え方や対策は、「当たり前」の集大成です。しかし、世の中で起きているサイバーセキュリティ被害は、ほとんどが「当たり前」の対策を怠ってしまったために発生しています。

「現実社会の一部」といえるほど国民一人ひとりの生活に浸透しているインターネットのサイバー空間では、残念ながら、条件が揃えば誰もがサイバー攻撃による被害を受けてしまう可能性があります。

サイバー攻撃による被害を受けないようにするためには、「当たり前」を忘れずに、国民一人ひとり全員が、自分にとってどんなセキュリティ対策が必要かを理解・実行する必要があります。

せっかくインターネットが普及して、より便利になったこの社会を壊さず発展させていくためには、多くの方々の協力が不可欠です。特定の誰かが黙っていても守ってくれるというものではなく、使う人もやらなきゃいけないことがあります。

### サイバー空間は現実世界のオプションではない



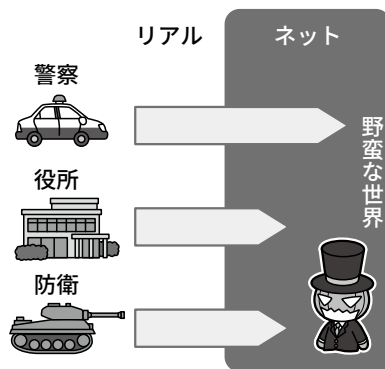
インターネット上のサイバー空間を、現実世界のオプションや便利な道具と捉える人もいますが、実際は現実世界の一部になり、国民生活に浸透しています。

### サイバー空間には「危険な世界」も残っている



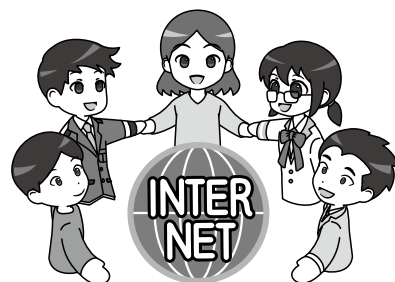
まだまだ未成熟な世界に人が進出して、社会のシステムや秩序の構築が間に合わない状態では、「力こそ正義」となりがちです。ある意味「生きぬく能力がない人には危険な世界」といえます。

### 現実世界と同じ「社会インフラ」がまだ整っていない



インターネットの世界には、さまざまなインフラが必要です。サイバー警察、電子政府、サイバー防衛、法制度などが次第に整いつつあります。しかし、よりよくしていくためには国民全体の協力が必要です。

### 全員がセキュリティ意識を醸成すれば安全・安心になる



みんながセキュリティを守ろうという意識を醸成することが、安全・安心なインターネットの利用を支えることにつながります。

本書も、そのようなことを前提に置いて、多くの方にお読みいただくことを想定して作られています。

本書を手がかりに、より多くの方

がインターネットを安全・便利に使うための知識を持つことができることを祈念しております。

- **.exe(エグゼ)**  
Microsoftが開発したファイル拡張子。Windows上で実行できるプログラムのファイル形式の1つ。Windowsが普及した結果、見た目に「.exe」を付け、利用者の目をごまかし、実際は不正なプログラムを潜り込ませるといった悪質な犯罪行為があるので注意が必要  
..... 141
- **00000JAPAN(ファイブゼロ ジャパン)**  
2011年3月11日の東日本大震災をきっかけに、日本国内での通信回線を、非常時に利用できる仕組みを整備し、緊急時におけるインフラ確保を目的に取り組みが始まったプロジェクト。2016年4月14日の熊本地震で初めて利用された。00000JAPANは、非常時下において、NTTドコモやau、ソフトバンクといった各キャリアの通信網を、臨時で認証なしに誰もが使えるようになる。利用時のSSID(無線LANの名前)が「00000」で始まっていることから、この名称となっている  
..... 90, 130
- **AES(エー・イー・エス)**  
暗号化方式の一要素。利用する無線LANの暗号化方式にAESという文字が入っている、WPA-PSK(AES)やWPA2-PSK(AES)という方式は、「暗号キー」を共有しない範囲では安全とされる。また、無線LANに限らずファイルや記憶装置の暗号化方式としても用いられ、数字+bitで記述される「鍵長」の数字が大きいくほど、不正な解読が困難とされる。WPA3はこれ以上の安全性を担保する  
..... 126
- **BCP(ビー・シー・ピー)**  
Business Continuity Planningの略。事業継続計画の意味で、災害時などの被害を最小限に抑えて事業を継続するために、あらかじめ人・モノ・金などのポイントから計画を立て、また、これを訓練することが望まれる。中小企業庁に詳細なウェブサイトがある  
..... 152
- **BEC(ベック)**  
Business Email Compromiseの略。ビジネスメール詐欺。攻撃者がビジネス用のメールを装い、企業の担当者をだまして、不正送金や機密情報の流出などが行われる攻撃  
..... 19, 50, 165
- **BIOSパスワード(バイオス・パスワード)**  
Windowsマシンなどで電源投入時に、OSが立ち上がる前に入力求められるパスワード  
..... 98
- **BYOD(ビー・ワイ・オー・ディー)**  
Bring Your Own Deviceの略。社員が個人の所有機材を会社の業務で使用する  
..... 152
- **CDN(シー・ディー・エヌ)**  
Content Delivery Network(コンテンツデリバリーネットワーク)の略。CDNをサービスとしているグローバル企業もある。写真や動画など、データサイズが大ききものをインターネットで通信すると、通信が遅延してしまう問題が発生してしまうため、遅延を解消する目的で作られた。CDNサービスでは、世界各地にデータセンターが展開されていて、データセンターのサーバーには一時的にファイルのコピーが保存されている。例えば、動画を配信する事業者がCDNを利用することで、事業者にとっては自社のサーバーへのアクセスを軽減でき、動画を視聴したいユーザーにとっては地理的に近いCDNサービスのサーバーからコンテンツを配信され、遅延なく安定的に動画を視聴できるメリットがある  
..... 167
- **DDoS攻撃(ディードスこうげき)**  
Distributed Denial of Service Attack。攻撃者などが不正に操作した多数のパソコンなどから、攻撃目標に一斉に多量の問合せなどを行い、攻撃対象の反応が追いつかず利用できない状況にする攻撃  
..... 21, 50, 70, 82, 104, 167
- **DMZ(ディーエムゼット)**  
DeMilitarized Zone。非武装地帯の意味。インターネットにつながるLAN用ルータに接続した機器のうち、LAN側ではなくインターネット側に設置したかたちにする仮想的なエリア。自前の公開用サーバやインターネット側から参照する監視カメラなどを設置する。DMZにあるIT機器はインターネットから直接見えるため攻撃されやすい  
..... 105
- **ECサイト(イーシー・サイト)**  
Electronic Commerceサイト。インターネット上にある商品販売店舗。オンラインショッピングサイト  
..... 87
- **FIDO(ファイド)**  
FIDO(Fast Identity Online:ファイド)は、新しい認証手段として期待されている技術の1つ。多くのサービス・アプリの認証手段にパスワードが利用されているが、セキュリティの確保の点で問題も見えている。2022年12月には多くの大手IT企業がFIDOを活用した「パスキー」採用の公表もあった。具体的には、使用するスマホとサーバの間でそれぞれ秘密鍵と公開鍵を持たせてユーザの認証を行い、パスワードを使用しない点が特徴  
..... 114
- **GDPR(ジー・ディー・ピー・アール)**  
GDPR(General Data Protection Regulation)とは、個人情報の保護やその取扱について、詳細に定められたEU域内の各国に適用される法令。2018年5月25日施行された。EU域内とはなっているが、インターネットの場合、国境の壁がないため、EU圏内のユーザからのアクセスを対象としたサービスやアプリの場合、GDPRの対象となることに注意  
..... 172

## ■ GPS(ジー・ピー・エス)

Global Positioning System。多数の人工衛星で構成される衛星測位システム。この衛星からの電波を使い計算を行うことで、現在地を測定することができる。主として米国が運用しているが、2018年春より日本版GPS「みちびき」が運用開始

..... 40, 66, 99

## ■ https://(エイチ・ティー・ティー・ピー・エス)

ホームページ(ウェブページ)にアクセスするためのURLの冒頭に記述される文字列。検索大手企業のGoogleが2014年ごろから積極的に安全なホームページへのアクセスを推奨し始め、2018年7月24日以降、https://でアクセスできるホームページ以外(http://ではじまるページ)については、警告を出すようにしました。詳しくは常時SSL化を参照

..... 163

## ■ ID(アイ・ディー)

機器やウェブサービスなどを利用するときに、利用者を識別する文字列。「ログインパスワード」とセットで、正統な利用者であることを証明する

..... 18, 32, 50, 72, 87, 110, 152

## ■ IMAP(アイマップ)

Internet Message Access Protocol。メールサーバからメールを受信するための通信上の規格。POPと異なるのは、サーバ上にメールを残した状態で管理できるので、ウェブブラウザがあればどこからでもアクセスできるウェブメールなどで使われることが多い。メールソフトでも利用可能。通常はVer.4のIMAP4が使われる

..... 138

## ■ IoT(アイ・オー・ティー)

Internet of Things。「モノのインターネット」ともいわれるが、あらゆるものをネットにつなげる考え方。しかし、IoT機器製造業者が全てネットワークセキュリティに詳しいとは限らず、攻撃者から見て乗っ取って踏み台にしやすい機器を増やす原因ともなっている

..... 17, 104, 111

## ■ JailBreak(ジェイルブレイク)

AppleのiPhone、iPadなどで規約に反した改造を行い、公式ストアでは認められていないアプリなどをインストールする行為。製造メーカーが設計したセキュリティ思想から逸脱し、マルウェアへの感染や乗っ取りなどの攻撃に遭う確率が高くなるため、大変危険な行為

..... 37

## ■ LTE(エル・ティー・イー)

Long Term Evolution。携帯電話の通信規格。携帯電話回線を提供する会社が個別に名称をつけている場合もあるが、主に4Gと呼ばれるタイプのものの総称。高速な無線通信回線ネットワークとしてWANと呼ばれることもある。さらに高速な5Gが登場しつつある

..... 99, 124

## ■ microSD(マイクロエスディー)

パソコンやスマホなどで使われる、小型のメモ리카ード。SDカードを小型化したもの

..... 42

## ■ NISC(ニスク)

National center of Incident readiness and Strategy for Cybersecurity。内閣官房内閣サイバーセキュリティセンターの略称

..... 28, 54, 120, 158

## ■ Office製品(オフィスせいひん)

Microsoft Officeなどに代表される、ワープロ、表計算、プレゼン用ソフトなどの総称

..... 30

## ■ OS(オー・エス)

Operating System(オペレーティングシステム)の略。パソコンやスマホの機器の上で動作し、利用者に操作のインターフェースを提供するソフトウェア。Windowsパソコンの「Windows」、Apple社パソコンの「macOS」、iPhoneの「iOS」、Androidスマホの「Android」などが代表的。ほかにも「Linux」(リナックス)という、サーバや工業機器、IoT機器などに搭載されているOSや、「UNIX」(ユニックス)、「Ubuntu」(ウブントゥ)などがある

..... 28, 98, 143, 158

## ■ PGP(ピー・ジー・ピー)

Pretty Good Privacyの略。米国の

Philip Zimmermannが開発した暗号化ソフトウェアの名称。公開鍵の交換を事前に当事者間で行い、その間で電子署名や暗号化されたメールのやりとりを可能にする仕組み

..... 139

## ■ PINコード(ピンコード)

狭い意味では、スマホなどを利用するときに打ち込む暗証番号のようなもの。複数回入力を間違えると明示的な入力遅延や入力画面がロックされるなどの規制がかかるものを指す。間違えすぎると強制的にデータを消去する「ワイプ」機能があるものも。本書では機器やサービス利用時に、4桁から6桁以上の数字で打ち込むもので、入力ミスでペナルティがあるものとして定義

..... 33, 78, 86, 92, 110, 153

## ■ POP(ポップ)

Post Office Protocol。メールサーバからメールを受信するための通信上の規格。IMAPと異なり、基本的にはメールをメールサーバからダウンロードして管理する。ただし、メールソフトの側で「メールサーバ」に残すという設定をした場合は、複数のメールソフトからダウンロードすることも可能。通常はVer.3のPOP3が使われる

..... 138

## ■ POSレジ(ポスレジ)

Point of Sales レジ。販売した段階でその情報が送信され、集中管理されるシステム。内部にはコンピュータが入っており、ネットに接続されているのでマルウェアに感染する事例もある

..... 17

## ■ QRコード決済

インターネット上で普及した電子マネーを、物理店舗での購買にも利用するための仕組み。使用する電子決済サービスごとに用意されたQRコードを利用し、スマホのカメラでそのQRコードを映し、電子マネーの支払い・受け取りを行う

..... 165

## ■ RMT(リアル・マネー・トレード)

Real Money Trade。ゲームなどで出現したレアな装備を、現実世界



の通貨で売買すること。ゲームの規約違反となっていることもある。また、販売に関して詐欺やさまざまなトラブルの発生もしている。レア武器は自力で出しましょう  
..... 69

## ■ root化(ルートか)

Android スマホなどで本来提供されていない、機器の管理者権限を奪取する改造。通常インストールできないアプリなどがインストール可能となる。これを行うことはメーカー本来のセキュリティ設計思想を逸脱しサイバー攻撃に弱くなるため、行ってはいけない  
..... 37

## ■ RSS(アール・エス・エス)

Really Simple Syndication もしくは Rich Site Summary の略。ウェブサイトの見えない部分で更新情報を掲載し、RSSリーダーで複数のサイトの更新情報を集約して見る事ができる。更新情報やタイトルだけでなく、仕様によっては要約文が提供される場合もある  
..... 159

## ■ S/MIME(エスマイム)

Secure / Multipurpose Internet Mail Extensions の略。電子メールのセキュリティの確保を目的とした暗号方式の1つ。電子証明書を用いてメールの暗号化とメールヘッダ署名を行える  
..... 139

## ■ SIM(シム)

スマホなどで携帯電話回線を利用するために挿入する小型のカード。電子的な eSIM もある  
..... 77, 84, 129

## ■ SIM認証(シムにんしょう)

公衆無線 LAN など、「暗号キー」を他人と共用しないように、それぞれの利用者によって異なる SIM の情報を使って認証を行う方式  
..... 126

## ■ SIMハイジャック(シムハイジャック)

スマホのインターネット通信や各種やりとりで使われる SIM カードを、悪意ある第三者が不正に則り、不正利用をすること。航空犯罪のハイジャックと同様に、SIM カードがかかわるすべてを奪ってしま

う行為からその名が付いている。SIM ハイジャック被害を受けると、スマホで利用されるネットバンキングなどまで被害が及ぶ、大変危険で悪意のある犯罪手法の1つ  
..... 85, 114

## ■ SIMフリー(シムフリー)

スマホなどの端末が、特定の携帯電話会社の SIM だけでなく、どの会社の SIM でも利用できるようになっている状態。逆に使えないように制限されている状態は SIM ロックという。ただし、SIM フリー端末であっても、どの会社の回線でも利用可能とは限らない。携帯電話会社が提供している周波数とスマホが使える周波数などが合っている必要がある  
..... 89

## ■ SMS(エス・エム・エス、ショートメッセージ)

Short Message Service の略。スマホなどで電話番号宛てで送受信できるテキストメッセージ。携帯電話回線契約があればデータ通信契約が無い状態でも送受信できる。一方、電話番号が無い場合や、データ通信専用 SIM で SMS が提供されていない契約では送受信できない。SMS がオプションとして提供されている場合もある  
..... 34, 83, 113, 163

## ■ SMTP(エス・エム・ティー・ピー)

インターネットで電子メールを送信するための仕組みの1つ。Simple Mail Transfer Protocol の略  
..... 138

## ■ SNS(エス・エヌ・エス)

Social Networking Service。会員制のサービスで、メッセージのやりとりやブログ風の発信などを行う。アカウントを作らないと閲覧できないものと、アカウントがなくてもウェブブラウザから閲覧できるものなど、さまざまな形態がある  
..... 23, 34, 51, 58, 80, 96, 118

## ■ SSD(エス・エス・ディー)

Solid State Drive。従来パソコンなどで用いられてきた大容量記憶装置であるハードディスク(HDD)に代わり、回転や可動部分がなく、電子的なメモリだけでこれを代替

する機器。HDD より小容量で比較的高価だが高速  
..... 42, 99, 112

## ■ SSID(エス・エス・アイ・ディー)

SSID (Service Selt Identifier) は、無線 LAN 接続の際に利用するネットワーク名のこと。無線 LAN 接続では、接続する無線 LAN アクセスポイントそれぞれを識別するために、最大 32 文字の英数字の名称を付ける  
..... 125

## ■ SSL(エス・エス・エル)

→ SSL/TLS

..... 132

## ■ SSL/TLS(エス・エス・エル/ティ・エル・エス)

Secure Socket Layer / Transport Layer Security。データを暗号化して送受信する方法で、SSL の方が古く、これを改訂して進化させたものが TLS。SSL が TLS の元になったこともあり、未だに SSL と呼ばれたり、SSL/TLS と書かれたりするが、古い資料やバージョンを明記しているものを除けば同義の意味と考えてよい  
..... 130

## ■ SSL証明書(エス・エス・エルしょうめいしょ)

SSL で通信を行うサーバの身分証明書のようなもの。認証局が審査を行って発行する。最近は審査がいい加減だったり、無料で発行する認証局の登場により、安全であることの目安とはならない状況になりつつある。より審査の厳しい EV-SSL 証明書も存在する  
..... 133

## ■ TKIP(ティーキップ)

Temporal Key Integrity Protocol。暗号化方式の1つ。無線 LAN アクセスポイントの暗号化方式にこの文字が入っていたら、危険と考え利用を避ける  
..... 126

## ■ TLS(ティ・エル・エス)

→ SSL/TLS

..... 132



## ■ TPMチップ(ティー・ピー・エムチップ)

Trusted Platform Module の略。TCG(Trusted Computing Group)と呼ばれる団体によって定義されたセキュリティの仕様に準拠したパソコンなどの内蔵記憶装置の暗号化を加速するチップ。「暗号キー」を秘匿し、本体が盗難された場合でも解読を困難にする。内蔵記憶装置だけが盗まれた場合は、TPMは本体に残るので「暗号キー」は秘匿され、当然解読がより困難になる

..... 99

## ■ UPnP(ユニバーサルプラグアンドプレイ)

Universal Plug and Play。ルータに内蔵されている機能で、家や会社のLAN側にある機器を、難しい設定抜きでインターネット側からアクセス可能にする。LAN内の機器がインターネット側からアクセスされ、「踏み台」にされることもあるので、利用しない方が安全

..... 105, 128

## ■ URL(ユー・アール・エル)

Uniform Resource Locator の略。http://やhttps://などから始まるインターネットのウェブサイトの住所を示す文字列

..... 37, 132, 163

## ■ USB(ユー・エス・ビー)

Universal Serial Bus。パソコンなどに周辺機器を簡単に接続するための規格

..... 156

## ■ USBセキュリティキー(ユー・エス・ビー・セキュリティキー)

USB端子に接続して、機器やサービスの正統な利用者であることを証明する物理的な鍵の役割を果たすもの、およびそこから認証用のワンタイムパスワードなどを送信するもの。BluetoothやNFCに使うタイプも存在する

..... 34, 113, 166

## ■ USBチャージャー(ユー・エス・ビー・チャージャー)

USB経由で機器を充電できるようにするためのもの。AC電源、乾電池や充電電池、車の電源ソケットを利用して充電できるものがある

..... 88

## ■ VPN(ブイ・ピー・エヌ)

Virtual Private Network。仮想プライベートネットワーク。業務用としてはインターネットを利用しながらセキュリティを守りつつ、独立したネットワーク間をLANのように接続する。一般の利用者用には、自分の機器からインターネット上の安全とされる出口サーバまでの区間の通信をすべてまるっと暗号化する

..... 54, 84, 130, 152

## ■ WAN(ワン)

Wide Area Network の略。LAN「Local Area Network」の対になる言葉。通信電波の供給範囲が広いものを指し、おもに携帯電話のLTEなどによる通信ネットワークなどを指す

..... 102

## ■ WEP(ウェッブ)

Wired Equivalent Privacy。暗号化方式の1つだが、容易に解読可能で安全ではない。無線LANアクセスポイントの暗号化方式にこの文字が入っていたら危険と考え利用を避ける

..... 126

## ■ Wi-Fi(ワイ・ファイ)

→無線LAN

..... 110

## ■ Wi-Fiルータ(ワイ・ファイ・ルータ)

ルータに無線LANアクセスポイント機能を付けたもの。無線LANアクセスルータ。→ルータ

..... 124

## ■ WPA(ダブリュー・ピー・イー)

Wi-Fi Protected Access。無線LANの暗号化方式の1つで、WPA-PSK(AES)と書かれたもので、「暗号キー」を他人と共有しない限り安全とされる。TKIPと入っていれば利用を避ける。公衆無線LANでこの方式を採用している場合は、「暗号キー」を他人と共有する場合もあるので注意

..... 126

## ■ WPA2(ダブリュー・ピー・イー・ツー)

Wi-Fi Protected Access 2。WPAをより強力にしたもので、AESが標準となった。「暗号キー」を他人と

共有しない範囲では安全とされている。もしTKIPと入っているものがあれば利用は避ける。公衆無線LANでこの方式を採用している場合、「暗号キー」を他人と共有する場合は危険

..... 126

## ■ WPA3(ダブリュー・ピー・イー・スリー)

Wi-Fi Protected Access 3。WPA2で近年発見された特殊な脆弱性や、その他無線LANにまつわる問題点の多くを解消する暗号化方式

..... 126

## ■ ZIPファイル(ジップファイル)

パソコンなどに保存されるさまざまなデータ(ファイルやフォルダ)を1つのまとまりにしたもの。ZIPと呼ばれる形式のため、ZIPファイルと呼ぶ。まとめることを圧縮、ふたたび分けることを解凍と呼ぶ。また、ZIPファイルに圧縮する際に、パスワードを設定して認証を必要とさせることも可能

..... 110

## ■ アウトソース

企業や組織において、プロジェクトの遂行やサービスの運用を内部の人材だけで対応するのが難しい場合、外部の人材、組織を利用することがある。これをアウトソース(人材の外部調達)と呼ぶ。インターネット関連のビジネスでは、サーバの運用そのものをアウトソースする場合が増えており、その際に利用されるものにクラウドサービスがある

..... 151

## ■ 悪意のハッカー

本書では「攻撃者」と同義。ハッカーやクラッカーなどとの使い分けはP.15参照

..... 28, 70

## ■ アクセスポイント

無線LANで通信するために、使用している機器を接続する先、およびその機器

..... 52, 127

- **アクティベーションコード**  
ソフトウェアをインストールしたり、コンビニなどで売っている、音楽サービスやゲームなどへのチャージカードを、利用可能にするために用いる。認証処理をするために入力時にネットに接続されている必要がある場合もある  
..... 51
- **アタッカー**  
→本書では「攻撃者」と同義。ハッカーやクラッカーなどとの使い分けはP.15参照  
..... 15
- **アップデート**  
セキュリティ改善要素が含まれているかどうかは関係なく、ソフトウェアやアプリの更新。アップデートを行うためのインストールファイルを「アップデートファイル」と呼ぶこともある。セキュリティの向上を含む場合もあるが、単に機能向上の場合もある。セキュリティ向上のみを行う場合は、セキュリティパッチと呼ばれる場合が多い  
..... 17, 28, 56, 96, 128, 157
- **アプリ**  
パソコンやスマホなどで、なんらかの機能を実現するプログラム。主にスマホで使われ、一部パソコンでも使われている名称  
..... 28, 53, 92, 113
- **アプリ連携**  
複数のアプリ間で機能を連携すること。カメラアプリにSNSアプリの投稿機能を連携し、カメラアプリから直接写真付き投稿を行えるようにするなど。権限を渡すことになり、攻撃者のサイバー攻撃の手口になるため利用は非推奨  
..... 106, 117
- **アンインストール**  
インストールしてあるプログラムやアプリを機器から削除すること  
..... 30, 56, 107
- **暗号化**  
文章などを正統な利用者以外通常の手段では読めないように加工すること  
..... 16, 33, 52, 86, 94, 110, 152
- **暗号鍵**  
暗号化処理(別項)において、データを暗号または復号する際に必要となる、短い符号のこと。暗号化処理で使用されるため、このような名前が付いている。暗号化処理の方法によって、共通鍵、公開鍵、秘密鍵といった種類がある  
..... 110
- **暗号化キー**  
暗号化と復号のために利用する鍵となる文字列。短く複雑でない暗号化キーは総当たりによって探り当てられやすい。また、なんらかの理由で流出したり、意図せず共有すると、キーを入手したのによって暗号化した内容が復号される。本書では「暗号キー」という  
..... 110
- **暗号化処理**  
パソコンやスマホでやりとりするデータに処理を加えることで、外部から判読できないようにすること。インターネットでのコミュニケーションが一般化している今、重要な情報を扱うデータには暗号化処理が必須となっている  
..... 99
- **暗号化チップ**  
暗号化をより高速に行うための、専用のチップ。≡TPM  
..... 99, 144
- **暗号化方式**  
暗号化の方式。一部の古い方式では「暗号キー」がなくても解読できるものもある。暗号化するときには利用する暗号化方式の安全性に注意が必要  
..... 94, 118
- **暗号化メディア**  
暗号化されたメディア。SSDやHDD、USBメモリなどのメディアを暗号化する  
..... 144
- **暗号キー**  
本書では暗号化と復号に使う鍵の名称として定義→暗号化キー  
..... 52, 94, 110
- **位置情報共有アプリ**  
現在、ほとんどのスマホに搭載されている位置情報特定機能を利用して、そのスマホのある物理的な場所(位置情報)を共有できるアプリ。家族や恋人、仲のよい友人間で、お互いの現在地を共有したい場合に利用される。最近では、こどもの通学時の安全確認といった利用方法にまで広がっている  
..... 75
- **違法アップロード・ダウンロード**  
イラストや写真、文章、ソフトウェアなど、著作権が発生する著作物を、著作者、著作権者に無断で利用したり複製し、インターネットを通じてアクセスできる状況に不正にアップロードすること。また、そのようにアップロードされた著作物を不正にダウンロードすること。その行為を行った場合、著作権法違反として刑罰の対象となる  
..... 68
- **インストール**  
プログラムやアプリを、スマホやパソコンに導入し、使える状態にすること  
..... 17, 28, 54, 84, 105, 137, 162
- **インターネットバンキング**  
インターネットを使って銀行の取引を行うサービス  
..... 51, 136
- **ウイルス定義ファイル**  
セキュリティソフトがマルウェアを検出するための定義情報が入ったファイル。実世界でいえば顔写真付きの手配書のようなもの  
..... 30
- **ウェブ**  
ウェブサイト、ホームページの略称。そもそもはインターネット上のウェブサイトを指す、World Wide Web(WWW,W3)の略  
..... 68, 134
- **ウェブサーバ**  
ネット上でウェブサイトを表示するためのサーバ  
..... 103, 132, 151
- **ウェブサイト**  
ネット上で文章ファイル風に情報を表示する場所。主としてウェブブラウザなどで閲覧する。ウェブサーバ上で運営される  
..... 37, 54, 72, 80, 115, 150

## ■ ウェブブラウザ

ネット上で公開されているウェブサイトを閲覧するためのソフトウェアやアプリ

.....30, 56, 103, 115

## ■ 炎上

SNSの投稿をきっかけに、想定外の情報拡散、また、不特定多数への反応が大きくなること。とくに悪い意味で使われる用語で、場合によっては投稿者あるいは投稿内容で指摘された人物や企業・組織への誹謗中傷につながり、一大騒動になる。炎上の範囲が大きくなると、その対象者・対象企業・対象組織の社会的立場を失わせるまでの事件にも発展する

..... 62, 157

## ■ オフラインアタック

攻撃者が暗号化されたデータなどを入手し、入力制限がない環境で解読攻撃を行うもの。主にネットに接続しないのでできる攻撃であり、オフラインという。＝オフライン攻撃

..... 112

## ■ オレオレ証明書

通信の暗号化に際し本来認証局に申請して発行してもらう証明書を、勝手に発行して暗号化通信に利用するもの。この証明書を利用しているウェブサイトにウェブブラウザでアクセスすると、警告が表示される。接続してはいけない

..... 134

## ■ オンラインアタック

攻撃者がウェブサービスなどに、不正にログインを試みる攻撃など。ネットを経由した攻撃が主なのでオンラインという。＝オンライン攻撃

..... 112

## ■ 鍵マーク

パソコンのブラウザでホームページにアクセスすると、上部にそのホームページのURLが表示される(https://の部分)。このとき、アクセスしたホームページが常時SSL化されていると、URLの頭に鍵マークが付く。つまり、このマークが付いているホームページは常時SSL化対応済み、と認識できる

..... 133

## ■ 拡散

インターネットやSNSにおける拡散とは、掲載された情報やSNSで投稿された内容が周囲に広がっていくこと。拡散の使われ方として、大切な情報や募金などの慈善行為を広げるための好意的な場合と、フェイクニュースや特定事物を攻撃する誹謗中傷をおもしろおかしく広げる、悪意が含まれる場合の2通りがある

..... 39, 53, 62

## ■ 拡張子

パソコンやスマホで利用するファイルの種類を識別するために使われる、ファイル末尾にある文字列。(ドット)の後ろにある1~4の文字列のこと。例えば、テキストファイルなら.txt、Excelファイルなら.xlsxとなる

..... 141

## ■ 管理者用パスワード

インターネット上のサービスや企業・組織内のサーバを管理するための権限を持つアカウントのためのパスワード。これを知っていると、該当するサービス・サーバのすべての作業が行える。なお、サーバ以外にも個人のパソコンやスマホでの設定もできる場合がある

..... 53

## ■ 記憶装置

パソコンやスマホの中にあるプログラムやデータを保存するメモリ。CPUに直結されデータをやりとりするメインメモリが主記憶装置、何らかの結線を使って接続しデータをやりとりするものが補助記憶装置という。ハードディスクやSSDなどはこれにあたる。総括して記憶装置

..... 42, 112, 168

## ■ ギブアンドテイク

ソーシャルエンジニアリングの手法で、相手になにかのメリットを与えることで、その代償として自分の目的の情報を引き出す手法

..... 22

## ■ 共通鍵暗号方式

通信を暗号化する仕組みにおいて、暗号化と復号に同一の(共通の)鍵を用いる暗号方式

..... 145

## ■ クライアント証明書認証

インターネットを通じてサーバにアクセスする際に、個人や組織を認証し発行される電子証明書。利用者側のパソコンやスマホにインストールされるものを指す。これと、サーバ側に置かれるSSLサーバ証明書が対となって、正しい利用者かどうかを認証し、不正アクセスを防ぐことができる

..... 129

## ■ クラウド

従来手元で保存していたデータなどを、インターネット上に存在しているサーバに保存し、ネットにつながったどの機器からでも利用できるサービス。ネットワークの図の上にインターネットを書く場合、雲(英語でクラウド)を書くことが一般的であったことから、インターネット上で提供されるサービスをクラウドサービス(略してクラウド)と呼ぶようになった。ほかにも「オンラインストレージサービス」と呼ぶ場合もある

..... 33, 63, 116

## ■ クラウドサーバ

インターネット上に存在する、データなどを保存しておくサーバ。おもに「機器の記憶装置と同等に利用できる」「特別なサービスを利用している意識はないが使えている」「でもどこにあるかわからない」雲のような存在感からCloudと呼ばれる。スマホなどでは、設定をよく確認しないと、知らないうちに、写真などのバックアップに使ってしまっていることもあるので注意

.....43, 85, 96, 148, 150

## ■ クラッカー

本書では「攻撃者」と同義。ハッカーやクラッカーなどとの使い分けはP.15参照

..... 15, 104



## ■ クラッキング

攻撃者が他者のアカウントや機器、サーバなどに不正に侵入すること。セキュリティを割って入るの「割る」のCrackから来ており、クラッキングを行う攻撃者をクラッカーとも呼ぶ

..... 15, 56, 70, 115, 157

## ■ 権限

Windows や macOS など、コンピュータ上で動く OS は、ログインする(使用する)ユーザごとに操作権限を指定できる。これを OS の権限と呼ぶ。例えば、管理者権限の場合、対象となる OS すべての操作が可能となり、データをすべて削除したり、OS そのものを再インストール(初期化)することが可能となる

..... 38, 156

## ■ 検体

セキュリティ会社などがセキュリティソフトでマルウェアを排除できるように、そのマルウェアを解析するための実物のサンプル

..... 48

## ■ 公開鍵暗号方式

通信を暗号化する仕組みにおいて、暗号化と復号に別個の鍵(手順)を用い、暗号化の鍵を公開できるようにした暗号方式

..... 139

## ■ 公開範囲

Facebook や Twitter などの SNS において自身の投稿内容を公開する範囲。また、クラウドサービスやプロジェクト管理ツールなどにおいても、サーバにアップしたファイルやサービス内の情報を公開する範囲を指す場合もある。公開範囲の名称はサービスによってさまざまだが、インターネット上すべてに公開する「全体公開」「一般公開」、SNS 上の友人やフォロワーまでの「友人までの公開」、さらにその友人やフォロワーまでの「友人の友人までの公開」、特定の人物を指定した「特定範囲での公開」「限定公開」などがある。ただし、公開範囲を限定したからと言って、公開範囲のユーザの行動によっては、その情報が完全に秘匿されるわけではないので注意が必要である

..... 60, 156

## ■ 攻撃者

悪意を持ってサイバー攻撃やそれに付随する攻撃を行うもの。悪意のハッカー。ブラックハットハッカーとも呼ばれる。本書では「ハッカー」そのものは悪意があるかどうかとは関係が無いので、とくに攻撃を行うものとして「攻撃者」とする。P.15 参照 = アタッカー。  
≡ クラッカー

..... 15, 28, 50, 86, 110, 150

## ■ 虹彩

目の中にある円盤状の膜で、人によって違っており、生体認証の要素として使われる

..... 34, 113

## ■ 公衆無線 LAN

街中や店舗などで、不特定多数に対してインターネット接続環境を提供する無線 LAN のこと

..... 124

## ■ 個人情報

生存する個人に関する情報で、氏名、生年月日、住所、顔写真など、特定の個人を識別できる情報を指す。日本では2005年4月から、個人情報の有用性を配慮しながら、個人の権利・利益を守ることを目的とした「個人情報保護法」が全面施行され、個人情報の取扱について一層厳格になった。また、この法令に基づき、個人情報の適正な取扱の確保を図ることを任務とする「個人情報保護委員会」が存在している

..... 34, 51, 60, 161

## ■ 個人情報保護委員会

個人情報保護委員会は、個人情報(特定個人情報を含む)の有用性に配慮し、個人の権利利益を保護するため、個人情報の適正な取扱の確保を図ることを任務とする、独立性の高い機関。個人情報保護法及びマイナンバー法に基づき、個人情報の保護に関する基本方針の策定・推進や個人情報などの取扱に関する監視・監督、認定個人情報保護団体に関する事務などの業務を行う団体

..... 169

## ■ サービス・アプリ連携

インターネット上のサービスやアプリが増えることで、1つのサービス、1つのアプリで閉じず

に、他のサービス・アプリと連動して操作したり、楽しめるケースが増えている。これを、サービス・アプリ連携と言う。例えば、Twitter を他のブログサービスとサービス・アプリ連携することで、Twitter で投稿した内容を、自動でブログサービスの方にも投稿できるようになる

..... 118

## ■ サービス連携

パソコンなどを使って複数のウェブサービスの間で連携をすることをサービス連携と呼ぶ。その中でとくにスマホ上でアプリによって連携をすることをアプリ連携と呼ぶ場合があるが、内容は同じ

..... 107

## ■ サイバー攻撃

インターネットを通じて、別の企業や組織、ときに国家を攻撃する行為の総称。対象は、パソコンやスマホといった個人が利用する1つの端末から、サーバやデータベースなどの大規模なものまで、手法によってさまざまある。ネット社会となった現代では、インターネット空間をサイバー空間と呼び、そこでの攻撃、すなわちサイバー攻撃を舞台とした国家間の争いが起きている事実がある

..... 29, 50, 63, 150

## ■ サイバープロパガンダ

SNS や ウェブサイト などのサイバー空間においてプロパガンダ(特定の思想・世論・行動を誘導する行為)を行うこと。インターネットが、人類の生活空間、社会として浸透した結果、国家間の争いの場所にもなった結果、生まれた事象。フェイクニュースやフェイクサイトを活用した方法など、悪質かつ狡猾な方法が増えている

..... 55



## ■ サプライチェーン

製品の原材料・部品の調達、製造、在庫管理、配送、販売、消費までの、製造から流通すべての流れを指す。大手企業が開発するスマホなどは、サプライチェーン管理がしっかりされていることが多い反面、その中の一部でのトラブル(自然災害・人工災害)により、製品の供給数への影響が大きくなるケースがある  
..... 160

## ■ 辞書攻撃

「ログインパスワード」などによく使われる文字列を集めて辞書化したものを使い、不正に他人のアカウントにログインできないかを試みる攻撃  
..... 32, 112

## ■ 常時SSL化

SSL (Secure Socket Layer) とは、インターネット上でデータを暗号化して送受信する仕組みの1つ。暗号化するだけではなく、電子証明書の利用により、通信者の本人性を証明することで、なりすましなどの不正利用を防ぐことができる。「https://」の項で説明したように、Googleの動きに追従する形で、今は多くのホームページ(ウェブページ)で、常時SSL化が推奨、一般化してきている  
..... 134

## ■ 情報モラル教育

インターネット普及がもたらした、爆発的な情報量の増加、また、インターネット上における年齢や経験、性別など制限のないコミュニケーションにおいて、社会規範を守るために行われる教育。技術の進化に合わせて価値観が変化するため、情報モラル教育自体が変化しており、それに追従していく必要がある  
..... 58, 168

## ■ 初期化

使用しているパソコンやスマホのハードディスクや保存スペースを、出荷状態と同じ状況にすること。その中に保存されているファイルやアプリはすべて削除される。なお、初期化方法によっては、データを復元できる場合がある  
..... 54, 97, 166

## ■ 初期パスワード

パソコンやスマホなどのログインに必要な機器で、出荷初期の状態で設定されているパスワード。初期パスワードは便宜上使われるため、利用者は入手後、必ず自身のパスワードに変更する必要がある  
..... 105

## ■ 署名アルゴリズム

安全な接続を行う際に利用されるサーバ証明書を確認するときに使用するもの。SHA-1/2、DESなどの種類がある。SSL化されたホームページへアクセスした際、そのページの証明書が正しいかどうか、署名アルゴリズムを見ることで確認できる  
..... 134

## ■ ショルダーハッキング

パソコンやスマホを操作している人物の背後から肩越し(ショルダー)に覗いて、無断でその人物の操作画面を盗み見し、さまざまな情報を盗んでハッキング(クラッキング)することからその名前が付いた。物理的な攻撃手法の1つ  
..... 29

## ■ スクリプトキディ

ハッカーのレベルになく、自分で作らず購入したマルウェアや簡単なスクリプトを使って悪事を働く、初心者攻撃者。「スクリプトを使うこども」の意  
..... 20

## ■ スタンドアロン

ネットワーク(つながっていること)と対になって使われる言葉で、ネットワークにつながっておらず単独で存在すること。ただし、ネットにつながっていて、かつ他の機能や機器と連携しないで動作する場合もスタンドアロンと表現する  
..... 33, 116, 168

## ■ ステルス状態

パソコンなどが起動していないように見えて、実際は動作している状態  
..... 99

## ■ スパイ

もともとの意味は、国家間などで秘密裏に動いて、敵対国や競争相手の情報を得る人物を指す。インターネットにおいては、その意味

を踏襲して、インターネットを通じて他のOSやアプリのセキュリティの不具合(セキュリティホール)を利用して、無断で侵入し情報を抜き取ることを意味する。また、そのアプリをスパイアプリ・スパイウェアと呼ぶ。多くのセキュリティ対策ソフトでは、既知のスパイアプリ・スパイウェアのチェックが可能で、侵入されている場合、検知可能となる  
..... 14, 40, 85, 108

## ■ スпамメール

もともとはインターネットの初期、不特定多数に対して多量に送られてきた広告メールなどの迷惑メールを指した。攻撃者がこの方法を用いてマルウェア感染などを狙う攻撃をしたり、詐欺サイトに誘導するフィッシングメールなどに利用することもある。この場合はスパムメールでありフィッシングメールでもあることになる。サイバー攻撃に用いられる場合は、特定の誰かを狙った少量の「標的型攻撃(標的型メール)」に対して不特定多数を狙うため「ばらまき型攻撃」と呼ばれることもある  
..... 29, 140, 161

## ■ スマートウォッチ

スマホと連動したり、単独でネットに接続してなんらかの情報をやりとりできる腕時計型の機器  
..... 40, 114

## ■ スマート家電

単独でネットに接続して、なんらかの情報をやりとりしたり、動作の指示を受け付けられる家電機器  
..... 31

## ■ スマートフォンを探す

Google アカウントに用意されている、使用しているスマホ(スマートフォン)を探す機能。対象となるスマホでログイン中のGoogle アカウントをインターネット経由で認識し、そのスマホの位置情報を確認できる  
..... 95

## ■ 脆弱性

＝セキュリティホール  
..... 18, 167

## ■ 生体認証

パソコンやスマホなどを利用する時の本人確認を、指紋、虹彩、静脈、顔の形など、本人の生体の一部分を用いて認証すること  
..... 28, 92, 113

## ■ セキュリティ・バイ・デザイン

インターネットやデジタルの普及、社会への浸透が進む中、企画・設計段階からセキュリティ仕様を準備し、セキュリティ確保を事前に意識して開発を進めるシステム開発手法。出来上がったものを守る、ではなく、あらかじめ堅牢なものを作る、という思想  
..... 150

## ■ セキュリティキー

無線LANに関するものの場合→「暗号キー」、物理的なものの場合→「USBセキュリティキー」  
..... 110

## ■ セキュリティソフト

パソコンなどのセキュリティを確保することに貢献するソフトウェア  
..... 30, 50, 74, 100, 134

## ■ セキュリティ対策プラン

パソコンやスマホなどのセキュリティを向上するために、複数の機能がパッケージになって携帯電話キャリアなどから提供されているもの  
..... 93

## ■ セキュリティパッチ

パソコンやスマホのシステム上に開いた、セキュリティの「穴」を塞ぐために、メーカーなどから提供される修正プログラム。パッチワークのパッチから来ている。アップデートファイルに含まれる場合もある  
..... 56

## ■ セキュリティホール

パソコンやスマホのシステム上、攻撃者が不正な侵入などを行える状態になっているプログラム上の「穴」のこと。＝脆弱性  
..... 17, 28, 53, 103, 137, 158

## ■ ゼロデイ攻撃

セキュリティホールが公になってから、メーカーなどがその穴を塞ぐための修正プログラムを提供するまでの期間に行われる攻撃。こ

の期間に攻撃を受けると、防ぐ手段はないため、利用者自身が「避ける手段」を講じる必要がある  
..... 39, 53, 106, 137

## ■ ゼロトラスト

基本は「決して信用せず、常に検証せよ」という考え方にもとづき、端末へのアクセスは、常に検証を行い、安全を担保し続けるモデルである。  
特定の製品を購入すれば導入できるというものではないため敷居は高いが、興味を持った方は、例えば独立行政法人情報処理推進機構から公開されている文書「ゼロトラストという戦術の使い方」([https://www.ipa.go.jp/icscoe/program/core\\_human\\_resource/final\\_project/zero-trust.html](https://www.ipa.go.jp/icscoe/program/core_human_resource/final_project/zero-trust.html))を参考に、自身の組織で導入できるかどうか検討してみしてほしい  
..... 151

## ■ 総当たり攻撃

攻撃者が「ログインパスワード」や「暗号キー」を破るために、全ての文字などの組み合わせを試す攻撃ブルートフォース攻撃、ブルートフォースアタックともいう  
..... 32, 111

## ■ ソーシャルエンジニアリング

対人(アナログ)、サイバーを問わず、人間の心の隙を突き、相手に自らの望むような行動をさせる心理テクニック。対人の代表的な例が「オレオレ詐欺」などの特殊詐欺、サイバーの代表的な例が「標的型メール」やBECなど  
..... 21, 47, 157

## ■ ソーシャルログイン

特定のSNSやウェブサービスのIDを使って、他のSNSやウェブサービスにログインして、利用可能にする規格。特定の身分証明書で、他のサービスを利用できるイメージ。新しいサービスを利用するために一からアカウントを作る手間を省くことができる。OpenIDとほぼ同義だが、他にもソーシャルログインに見える機能は存在する。鍵となるアカウント情報が流出すると連鎖的に乗っ取られるため、本書では非推奨  
..... 117

## ■ ソース

「情報ソース」の意味で、発信された情報の発信元。発生した事象そのものを明確に見たり聞いたり体験した上で発信しているものを一次ソースという。伝言などで発信しているものを二次ソース、三次ソースと呼び、次第に信憑性が低くなったり、本来の意味とは別の意味で使われている可能性が高くなる。なお、プログラムを作るための設計ファイルもソース(もしくはソースコード)と呼ばれる  
..... 71, 158

## ■ ソフト

ソフトウェア(≡プログラム)の略。対になる言葉は機器を意味するハード(ハードウェア)  
..... 116, 151

## ■ ソフトウェアトークン

多要素認証などで使われる使い捨てパスワード(ワンタイムパスワード)を出力するトークンを、ソフトウェアで実現しているもの。例えばソフトウェアトークンを出力するスマホ用アプリ  
..... 34, 113

## ■ ダークウェブ

ダークウェブとは、日常的に利用されているウェブサイトと異なり、匿名性の高いネットワーク上に構築された、主として犯罪や国家間の争いに利用されるウェブサイトの総称。GoogleやYahoo!などの検索エンジンでは見つけれず、特別な条件でアクセスできるURLやアクセス方法が紹介される  
..... 52, 70, 161

## ■ 多要素認証

サービス利用時に行う利用者認証を、3つの要素(①知っているもの②持っているもの③本人自身に関するもの)のうち、2つ以上の要素を用いて行うもの。3つの要素すべてを使う場合などもあり得る  
..... 28, 51, 92, 113, 164

## ■ チート行為

ゲームなどで本来認められた方法ではなく不正な方法によるプレイ。また、はそれによって利益を得る行為  
..... 69

## ■ 中間者攻撃

インターネット上の通信において通信している2者の間に入り、両者がやりとりする情報のすり替えやなりすましにより、情報の盗聴、不正利用など、通信上で悪意ある攻撃を行う手法。保護されていないインターネット回線など、信頼できない通信経路上で被害に合う可能性が高くなる

..... 165

## ■ 著作権侵害

イラストや写真、文章、ソフトウェアなど、著作権が発生する著作物において、著作権を保持している人物の権利を侵害すること。不正コピー、違法アップロード・ダウンロードなどがその対象となる。オンライン・デジタルにより、誰もが複製しやすくなったため、著作権の管理が非常に重要な一方で、その利便性を活用するために、著作権フリーやクリエイティブ・コモンズ・ライセンスといったものも存在する。また、著作権などが発生しないパブリックドメインでのコンテンツ流通も行われている

..... 68, 170

## ■ 通信の秘密

個人間の通信の内容およびこれに関連した一切の事項について、公権力や通信当事者以外の第三者がこれを把握すること、および知り得たことを他者に漏らすなどを禁止すること。通信の自由の保障と対で考える必要がある

..... 139

## ■ 通知ウィンドウ

パソコンなどで、なんらかの通知を出す表示のこと

..... 41

## ■ 通知機能

エラー発生、メール受信、その他のアラートなどを利用者に通知する機能

..... 41

## ■ 使い捨てパスワード

多要素認証などで用いられる、利用するたびに更新されるパスワード。＝ワンタイムパスワード

..... 118

## ■ 使い捨てメールアドレス

メールアドレスを利用する場合、

多くの利用者は自分用として使い続ける。しかし、最近では、フリーメールサービスなどで、1回だけ使うメールアドレスなどが入手しやすくなっており、これを使い捨てメールアドレスと呼ぶことがある。継続的に利用しない場合は便利だが、使い捨てメールアドレスを利用したインターネット犯罪も横行しており、注意が必要

..... 142

## ■ ディクショナリアタック

→辞書攻撃

..... 112

## ■ データ消去機能

パソコンやスマホを買い替えた場合、古い端末を廃棄したり、転売することがある。その際、その端末内に含まれているデータが完全に消去されていないと、次に渡った相手に不測の使われ方をされる危険がある。その場合、端末に含まれるデータを完全に消去できるのが、データ消去機能である。端末にあらかじめ用意されている場合もあるが、ない場合、別の専用アプリを別途入手する必要がある

..... 97

## ■ データの移行

スマホの機種変更をはじめ、使用している端末を替える際に、それまで使用していた端末に残っているデータを、新しい端末へ移すこと。最近のスマホでは、まったく同じ状態でのデータ移行がしやすくなっている。ただし、端末に紐づくデータは移行できないものもある

..... 96

## ■ データローミング

ローミングに関して、データ通信のローミングを行うこと

..... 77, 87

## ■ テザリング

パソコンなどで、スマホなどを経由してインターネット接続をする方法。スマホをルータとして利用する方法など

..... 130

## ■ デジタル署名

公開鍵暗号技術を利用して、セキュリティ性を担保した署名のこと。暗号技術を利用していることで、

安全性が高く、電子契約サービスと合わせて利用することで法的な効力も持つ

..... 140

## ■ デジタル遺産

利用者が持っている、デジタル形式の財産の総称。その中には、デジタルコンテンツや電子マネー、さらに暗号資産といった貨幣価値に直接つながるものから、SNSアカウントなど利用者自身の無形の価値までを含む。インターネットが浸透した今、このデジタル遺産の扱いと、利用者の死後を想定した管理についての議論が進んでいる

..... 78

## ■ テレワーク

進化したコンピュータや通信インフラなど情報通信技術を活用した働き方の総称。従来は、会社(オフィス)へ集まって業務を行うが、テレワークの場合、自宅や別の場所からインターネットを通じて連携を取って業務を遂行できるため、時間や場所を有効活用できる。リモートワークと呼ぶ場合もある

..... 151

## ■ 投資詐欺

株などの金融により、将来に向けた資産を増やすために行う投資にまつわる勧誘や、実際の架空投資などを行う詐欺。インターネットバンキングやインターネット投資がしやすくなったことで、投資詐欺の幅が広くなり、被害件数が増えている

..... 165

## ■ ドライブバイダウンロード攻撃

いずれかのウェブサイトを訪れただけで、なんらかのプログラム(この場合はマルウェア)のインストールが発生する攻撃

..... 56



## ■ トラッシング

ゴミ箱に捨てられた紙などから重要な情報を探し出すソーシャルエンジニアリングのテクニック

..... 22

## ■ 内閣サイバーセキュリティセンター

正式名称は「内閣官房内閣サイバーセキュリティセンター」。日本政府のサイバー政策の策定や政府機関へのサイバー攻撃の検知と調査を行っている機関。国民へのサイバーセキュリティ意識の啓発も行う。通称 NISC。間違われやすいが内閣府ではない

..... 28

## ■ なりすまし

サイバーセキュリティにおける「なりすまし」とは、悪意ある人物が、別の人物になりすましてパソコンやスマホ、システムを利用し、不正な行為を行うことを指す。なりすましをされた人物は、自分がまったく意図しない操作やコミュニケーションを行われ、ときに犯罪に巻き込まれる場合がある

..... 47, 51, 62

## ■ 二段階認証

利用者認証を2回に分けて行うもの。多要素認証と異なり、同じ認証の要素で2つの段階に分けて認証する場合もそう呼ぶ。一方、異なる要素を組み合わせで2回認証を行う場合は二要素認証とも呼ぶ。同じ要素2回よりは異なる要素2回の方がセキュリティレベルは高くなる

..... 114

## ■ 認証局

申請に基づき SSL 証明書の発行を審査する機関

..... 133

## ■ ネームドロップ

業務上の上司や立場が上の人間を装って要求を実行させるソーシャルエンジニアリングの手法

..... 22

## ■ ネットワーク暗証番号

通信事業者のサービスを利用する際に、利用者が本人であることを認証するための暗証番号

..... 110

## ■ ネットワークカメラ

主にネットワーク上に設置された監視カメラ。セキュリティ上は主にインターネット上から直接存在が見えるものを指し、サイバー攻撃の対象となりやすい。IP カメラとも呼ばれる。IoT 機器

..... 31

## ■ ネットワークキー

無線 LAN でアクセスポイントへの接続や通信の暗号化に使われる鍵。本書では「暗号キー」に分類している

..... 110

## ■ ネットワークルータ

家庭内や会社内の LAN をインターネットに接続するための窓口的役割を担う機器。無線 LAN 機能を内蔵している場合は「無線 LAN ネットワークルータ」「無線 LAN アクセスルータ」と呼ばれる

..... 17

## ■ 野良 Wi-Fi(のらワイファイ)

野良猫のように誰が設置したか分からない無線 LAN アクセスポイント。主に暗号化されておらず誰でも利用できる状態になっているもの。暗号化されていない時代に設置されてそのままのものもあるが、攻撃者が情報を詐取するために設置しているものもある。災害時や観光目的に、運営主体がはっきりして設置される暗号化無しの無線 LAN アクセスポイントは別

..... 136

## ■ バージョンアップ

アップデートファイルなどを適用して、ソフトウェアやアプリのバージョンが向上すること。セキュリティ関係の更新が含まれることもあり、積極的に適用するべきもの。バージョンの整数が上がるものをメジャーアップデート、小数点以下が上がるものをマイナーアップデートなどと呼ぶ

..... 30

## ■ ハードウェアトークン

多要素認証などで用いられる使い捨てパスワードを、専用の物理機器として提供するもの

..... 34, 113

## ■ パクリ

別の人物が作成したさまざまなコンテンツを真似ること。パクリの表現が使われる場合、多くが無断で真似て、ときにまったく同じ状態で複製し利用する状況となり、元コンテンツに対する著作権侵害となることが多い。ロゴやウェブページの雰囲気(トーン & マナー)など、見た目でわかりやすいものの場合、炎上につながりやすい

..... 68, 170

## ■ パスコード

一部のアプリなどで PIN コードと同じ役割をするものを指す言葉

..... 110

## ■ パスフレーズ

パソコンやスマホ、あるいはそれらで動くアプリや各種インターネットサービスを利用する際、必要となる認証で利用するパスワードのこと。パスフレーズとは、文字数が多いものを指す

..... 110

## ■ パスワード

利用しようとしている人が、その機器やサービスの正規の利用者であることを証明する、合い言葉のような文字列。本書で言う「ログインパスワード」のみを指す場合と、暗証番号(PIN コード)などや無線 LAN を利用する時に入力する「暗号キー」を含む場合がある。本書では明確に分けて記述している

..... 16, 28, 50, 61, 84, 92, 110, 152

## ■ パスワード管理アプリ

インターネット上のさまざまなツールやサービスを利用するにあたり、ログイン情報の管理が煩雑化している。それを解消するのがパスワード管理アプリ(パスワードマネージャー)である。1つのアプリの中で、各ツールの ID とパスワードを管理するもので、ID とパスワードを確認するにあたって、生体認証や二段階認証を利用することで、セキュリティを確保する

..... 33, 78, 153



## ■ パスワードの使い回し

パソコンやスマホ、あるいはそれらで動くアプリや各種インターネットサービスを利用する際、必要となる認証で利用するパスワードを使い回すこと。1つのパスワードをさまざまなところで使い回すと、万が一そのパスワードが、悪意ある利用者に漏洩した場合、すべてのアプリで不正利用される危険があるため、パスワードの使い回しは避けなければいけない

.....35, 51, 61, 164

## ■ パスワードリスト攻撃

→リスト型攻撃

.....112

## ■ パターンロック

スマホをロック解除するときに、画面上に表示される複数の点を、あらかじめ登録したパターンでなぞり、ロックを解除する機能

.....40, 92

## ■ ハッカー

コンピュータに精通し、その方面の高い知識と技術を持つ人を指す尊称で、イコール悪事を行う攻撃者ではない。ハッカー、攻撃者、クラッカーなどの使い分けはP.15参照

.....15

## ■ バックアップ

パソコンやスマホの情報を別途保存しておき、機器が故障したり紛失や盗難したりした場合に、復元するためのもの。機器の情報の一括バックアップと、目的のデータ毎のバックアップがある。更新された部分だけを追加してバックアップしていく方式は「差分バックアップ」とも呼ばれる

.....29, 54, 63, 95, 115, 153

## ■ バックドア

機器やシステムに設けられた、正規のログイン方法ではないアクセス方法。攻撃者がシステムに侵入して、再度侵入するために不正に設置する場合や、システム開発者や管理者が管理の手間を省くために設置し、正規のリリース後それをわざと残したり忘れたりしている場合もある

.....160

## ■ パッチ

≒セキュリティパッチ

.....56

## ■ パラメータ

機器やソフトウェアの設定上の要素

.....139

## ■ ハリーアップ

ソーシャルエンジニアリングの手法で、相手を急かすことで正常な判断をできなくなるようにして、目的の要求を通すこと

.....22

## ■ 秘密の質問

ウェブサービスなどでパスワードを忘れてしまい、再度パスワードを設定し直すときに本人である確認をするため、あらかじめ設定しておく質問。ただし、質問はサービス側が用意したものがほとんど個人情報にまつわるもののため、正直に答えているとSNSなどで探し当てられることもある

.....34

## ■ ヒューミント

スパイの諜報活動で、ターゲットの交友関係などを調査すること

.....108

## ■ ヒューリスティック分析

手配書方式のマルウェア検知方法を避ける攻撃が普及してきたため、マルウェアのプログラム上の特徴ではなく、マルウェアの挙動によって判断する方法。別称「ふるまい検知」

.....48

## ■ 標的型メール

攻撃者がターゲットを定めて、マルウェアなどに感染させるために、個人宛のフィッシングメールを送り付けてくる攻撃。ターゲットの名前だけでなく、業務上のメールと見分けがつかない内容や、場合によっては業務上の付き合いがある人間の名前、あるいはその人間のメールソフトを乗っ取って送られてくることもある

.....17, 29, 142, 162

## ■ ファームウェア

利用する機器のソフトウェアやアプリではなく、機器自身を動かすプログラム。ソフトウェアやアプ

リだけでなく、更新されたら必ずアップデートしなければならないもの

.....30, 104, 127

## ■ ファームウェアパスワード

パソコンの電源投入時に入力求められるパスワードの名称の1つ。これを入力しないと、そもそも起動することができない。≒起動パスワード ≒ BIOSパスワード

.....98

## ■ ファイアウォール

パソコンなどのネット接続部に存在するプログラムで、内部から外部へのアクセスは通し、外部からの不正なアクセスを防ぐ壁の役割をする。また、企業などでは専用の機器として存在する

.....46

## ■ フィッシングメール

攻撃者がターゲットから、お金につながる情報や個人情報を盗み取るための詐欺メール。フィッシング(phishing)は洗練された(sophisticated)＋釣る(fishing)から来ている。嘘の情報を餌にして釣り上げるというイメージ

.....39, 137, 160

## ■ フィルタリングサービス

青少年がネットにアクセスするに当たって、不適切なウェブサイトを閲覧しないようにするサービス

.....64

## ■ フェイクニュース

SNSが普及してから爆発的に増えた、他人や社会に悪い影響を与える偽りの情報。最近では、企業や組織の公式情報、著名人の宣伝、さらには政治を含めた国家のメッセージなどでSNSが活用されることが増え、その状況を逆手に取って、悪意あるユーザがフェイクニュースを作成・発信し、自身の承認欲求を満たしたり、対象となる人物・企業・組織・国家などに情報面での攻撃をするケースが増えている。フェイクニュースに惑わされないよう、日本ではさまざまなレベルでのリテラシー教育(情報モラル教育)へ注力しはじめている

.....55, 71

## ■ 復元

誤って削除・消去してしまったデータや、事故・トラブルによって消去されたデータを、再びできるようにすること。通常、削除・消去したデータは復元が難しいが、最近のパソコンやスマホでは、削除したデータを一定期間保存して、その期間内であれば復元できる場合がある。なお、パソコンやスマホの本体が故障して消えたデータの復元は、ほぼ不可能となる  
..... 29, 166

## ■ 復号

暗号化されたデータを、暗号キーを使って元に戻すこと  
..... 54, 110

## ■ 不正アクセス

企業や組織で管理されているサーバや、各種インターネットサービスにログイン権限のあるユーザではない、悪意のある別のユーザが不正な方法を使ってログインし、アクセスすること。不正アクセスが行われると、そのサーバに置かれているさまざまなデータや、正規のユーザの個人情報などが抜き取られる危険がある。日本では、2000年2月に施行された不正アクセス行為の禁止等に関する法律(不正アクセス禁止法)により、法律で固く禁じられている  
..... 34, 70, 164

## ■ 不正アクセス通知

利用しているウェブサービスなどに、不正なアクセスが試みられると、スマホなどに通知が送信されてくるサービス  
..... 46

## ■ 不正コピー

著作権が発生する著作物(イラストや写真、文章、ソフトウェア)で、かつ、複製が禁じられているあるいは通常の利用方法では複製ができない状態のものを、不正に、あるいは、不正な手段を使ってコピー(複製)すること  
..... 69

## ■ 不正送金

インターネットバンキングにおいて、悪意ある人物が、別の人物の口座および預金を無断で利用して送金する犯罪行為。インターネットバンキングの利用者が増えた

2010年代中盤から、その被害は増え続けている。不正利用に至るケースとして、利用者のパソコンやスマホに侵入するマルウェアの感染、また、迷惑メールを経由したフィッシング詐欺など、多様化しており、インターネットバンキングをの利ユーザーは注意が必要である  
..... 51, 70, 165

## ■ 不正ログイン

パソコンやスマホの起動、また、その後の各種アプリケーションの使用開始時においてID(アカウント)とパスワードを利用してログインする際、本人以外の悪意ある第三者が勝手にログインする行為。最近では、OSやアプリケーション側でログイン場所やログイン端末を確認し、通常使用されている場所や端末と異なる場合に、注意喚起(アラート)を出すことで、不正ログインの被害を軽減する仕組みが用意されている  
..... 166

## ■ 踏み台

攻撃者がサイバー攻撃を行う際、正体を隠すためにコントロール下においたパソコンなどを一旦経由すること。≡ゾンビ化  
..... 50

## ■ 不明なアプリ

パソコンやスマホで利用できるOSと、その上で動くアプリに関しては、OS提供側で許可を得られたものを正式なアプリとして利用できる。しかし、中には許可を得ずに提供したり利用できるアプリがある。これを不明なアプリと呼ぶ。なお、スマホの場合、iOS・Androidとも、世の中に公開する場合は、それぞれApple・Googleの審査を通ったものしか配信できない  
..... 38

## ■ フライトモード

スマホなどを飛行機で移動中に使えるように、外部に電波を飛ばない状態にするモード。それに伴い電池の消費が少なくなるので、災害時の省電力モードとしても利用できる  
..... 81

## ■ ブラウザ

→ウェブブラウザ  
..... 33, 134, 152

## ■ ブラウザ版

SNSなどで、アプリではなくウェブブラウザを使ってアクセスするために提供されているもの  
..... 56, 103

## ■ フリーメール

無料で提供されるメールサービス。広告などが表示されるか、利用者の利用情報を提供する代わりに無料で利用できる  
..... 138

## ■ フレンドシップ

ソーシャルエンジニアリングのテクニック。友情を持って接することで要求を断りにくくする  
..... 22

## ■ プロダクトキー

OSなどをインストールするとき、正統な利用者であることを証明するための文字列。パソコンにインストールされた状態で販売されるものは本体にシールで貼ってあり、店頭などで単体で販売される場合はパッケージ内部に封入されている。紛失すると再インストールすることができなくなる  
..... 98

## ■ プロバイダ

インターネットの接続環境を提供する企業。インターネット回線と提供する企業が同一の場合と、別々の場合がある  
..... 63, 93, 125

## ■ ベンダー

ソフトウェアやハードウェアなどの製品を販売する企業  
..... 38

## ■ ポート

パソコンやスマホがネットを通じて相手とデータを送受信するための窓口。それぞれに数字が振られ、これを「ポート番号」という。また、送信するものを「送信ポート」、受信するものを「受信ポート」と呼ぶ  
..... 132

## ■ ホームページ

=ウェブサイト  
..... 18

## ■ 補助記憶装置

CPUにケーブルなどを介して接続されデータを記録する記憶装置。ハードディスクやSSDなど。これに対してメインメモリと呼ばれCPUに直結するものを主記憶装置という。→記憶装置

..... 42, 112

## ■ ホスティングサービス

ホームページなどを開設するウェブサーバやメールサーバなど、各種サーバを運用するためのスペースを提供するサービス。ホスティングサービス事業者が運営するサーバを利用することで、自身でサーバの管理をする手間が省ける。個人向け、企業向けなど、用途に応じた種類やプランがある

..... 167

## ■ ボット

ロボット(robot)の短縮形。さまざまな作業を自動化したプログラムのことでTwitterで自動的に呟くものがある。「悪意のボット」となると、パソコンやIoT機器などを乗っ取ってゾンビ化するためのプログラムを指す

..... 16, 50

## ■ ボットネット

悪意のボットにコントロールされた機器で構成される集合体。パソコンやIoT機器などの機器が、コントロール用のサーバによって管理され、DDoS攻撃などに利用される

..... 30, 50, 104

## ■ マネタイズ

なんらかの手段で得たモノや情報、システムをお金に換えたり、それを用いて稼いだりすること

..... 146

## ■ マルウェア

攻撃者が目的とする機器を攻撃するために利用する不正なプログラム

... 16, 29, 50, 59, 86, 100, 115, 152

## ■ マルバタイジング

マルウェアを含んだ広告を用いるサイバー攻撃。攻撃者がウェブサイトを開覧したものを感染させるために広告ネットワークにお金を払って出稿する

..... 137

## ■ 水飲み場攻撃

攻撃者が目的とする相手(個人もしくは企業の社員など)を、マルウェアに感染させるために、あらかじめ訪問しそうなウェブサイトにもマルウェアを仕込んで待つこと。砂漠などで動物が水があるところによってくる様子からつけられた

..... 56, 137

## ■ 無線LAN

ネット で用いられる通信に、無線の信号を用いるもの。LANはLocal Area Networkの略で、通常は会社や家など小さい単位で用いる。インターネットとはルータを境にネットワーク的には分離されている(データの行き来は可能)。「Wi-Fi」とも呼ぶこともある。これに対して広範囲を対象とするネットワークはWAN(Wide Area Network)と呼ぶ

..... 31, 86, 94, 111, 152

## ■ 無線LANアクセスポイント

無線LANを利用するために、無線LANアクセッスルータによって提供される接続環境、もしくはその機器。本書では環境を指している

..... 52, 86, 124

## ■ 無線LANアクセッスルータ

無線LANアクセスポイントを提供する機器

..... 17, 124, 157

## ■ 迷惑メール

受け手が求めず、勝手に送りつけられる電子メールの総称。迷惑な電子メール、ということでその名が付く。迷惑メールには、広告宣伝を目的にしたものから、詐欺犯罪目的の「下級請求メール」や「不当請求メール」、さらにネット攻撃を目的とした「ウィルスメール」など、さまざまなものがある

..... 37

## ■ メッセンジャーアプリ

利用者同士でコミュニケーション(メッセージのやりとり)をするためのアプリ。メールよりも手軽で、簡単に会話できるのが特徴。日本ではLINEを筆頭に、テキストでのコミュニケーションに加え、スタンプを利用したメッセージのやりとりが増えている

..... 75

## ■ ランサムウェア

パソコンやスマホなどのファイルを暗号化したりロックしたりして使えなくし、「解除してほしいかったら身代金(ransom)を払え」と要求してくるマルウェア

..... 16, 29, 54, 70, 100, 166

## ■ リカバリ

コンピュータを利用している最中に、ハードウェア以外の部分、OSやファイルが破損し、データが使用できなくなる場合がある。このとき、リカバリという手法により、OSやファイルの復旧ができる可能性がある。最近ではこれらを行うリカバリツールが存在する。また、企業などでは重要なデータに関して「バックアップ」という複製を用意し、トラブルで破損した場合に、バックアップからリカバリすることが一般化してきている。そのほか、コンピュータに限定せず「回復する」「復旧する」といった意味・ニュアンスで使用される

..... 150

## ■ リカバリメディア

あらかじめOSがインストールされたパソコンで、不具合が起きたときのOS再インストールのため、購入後作成するべきインストール用のメディア

..... 98

## ■ リスト型攻撃

ウェブサービスなどから流出したパスワードのリストなどを使って、他のサービスでログインを試みる攻撃

..... 32, 111

## ■ リモートロック

ノートパソコンやスマホなど持ち運びで使う端末を、遠隔操作してロック(操作を受け付けられない状態にする)こと。端末のOSやアプリケーションによって操作方法はさまざま。使用している端末を紛失した際には、まずリモートロック機能を利用して、悪意ある操作から守ることが必要

..... 94

## ■ リモートワイプ

遠隔操作でスマホやパソコンの自身を消去すること

..... 94, 144

## ■ リンク

ウェブサイトやメール中にある、クリックすると所定のウェブサイトにジャンプする(リンクする)状態に設定されている文字列をさす。有意な文字列に設定されている場合もあれば、リンク先のURLの文字列に設定されている場合もある。表示されているURLとは別の場所へのリンクを設定できるため、表示されているものがイコールリンク先だとは思わないこと

..... 18, 36, 54, 115, 157

## ■ ルータ

インターネットなどを利用するために利用者が接続・経由する機器。会社や家庭で利用する無線LANアクセッスルータの他、高速なWANの回線を利用して、主に屋外などでノートパソコンなどを接続して利用するモバイルルータがある。また、有線だけで利用する有線ルータもある

..... 103, 111

## ■ ローミング

携帯電話などを海外で使用する時、その国の携帯電話会社と別途契約を結ばないまま、音声通話を利用できる状態にすること。同様のことをデータ通信に対して行う場合は「データローミング」という

..... 84

## ■ ログ

その機器で行われた活動を記録したデータ。通信に関するものは「通信ログ」という

..... 46

## ■ ログアウト

機器やサービスの利用している状態を終了すること。ウェブサービスの場合、利用していたウェブブラウザを終了してもログイン状態は継続される場合があるので、明示的にログアウトの操作をする必要がある

..... 97

## ■ ログイン

機器やサービスに接続し、パスワードなどを入れることで利用できる状態にすること

..... 28, 50, 72, 96, 111, 157

## ■ ログインパスワード

本書では機器やサービスを利用状

態にするために入力するパスワードとして定義

..... 98, 110, 169

## ■ ロック

攻撃者による不正なログインなどが試みられ、機器やウェブサービスへログインできなくなった状態。また、自らの機器を紛失したときに、誰かが勝手に操作できないようにした状態。これを遠隔操作で行うことを、リモートロックや遠隔ロックという

..... 29, 77, 92, 110

## ■ ロック画面

スマホを他者が勝手に操作できないような状態にした画面

..... 41

## ■ ワイプ

携帯電話やスマホのデータを消去すること。英語のwipe(拭きとる)という意味から、きれいにすることでそのように使われるようになった。最近のスマホやタブレットのOSでは、遠隔操作でワイプするリモートワイプの機能が搭載されていることが多く、紛失・盗難のあった端末のデータを遠隔地から消去することで、データの流出リスクを軽減できる

..... 111

## ■ ワンタイムパスワード

=使い捨てパスワード

..... 84, 113



## NISC 関連ウェブサイト、SNS 一覧

### ■ 内閣官房内閣サイバーセキュリティセンター(NISC)公式ウェブサイト



<https://www.nisc.go.jp/>  
日本政府のサイバー政策の策定や政府機関へのサイバー攻撃の検知と調査を行っている機関。国民へのサイバーセキュリティ意識の啓発も行う。通称「NISC」。

### ■ みんなで使おうサイバーセキュリティ・ポータルサイト



<https://security-portal.nisc.go.jp/>  
NISCが運営する、サイバーセキュリティ関連の情報を発信する普及啓発用サイト。本ハンドブックの配布も行っている。

## NISCのSNSによる情報発信

### ■ Twitter

#### 内閣サイバー(注意・警戒情報)



@nisc\_forecast

フィッシング詐欺・マルウェアなどの注意喚起情報やソフトウェアの更新情報を発信している。

### ■ Twitter

#### 公式アカウント



@cas\_nisc

NISCの取組やサイバーセキュリティに関連する情報を発信している。

### ■ Facebook



<https://www.facebook.com/nisc.jp/>

NISCの活動の紹介や、サイバーセキュリティに関するお役立ち情報を原則1日1回、コラムの形で発信している。

### ■ LINE

#### セキュリティ関連情報



LINEID: @nisc-forecast

原則1日1回、サイバーセキュリティに関するお役立ち情報をコラム形式で発信している。

# 索引

## アルファベット

BYOD .....	154
CTF .....	184
CYDER .....	184
DDoS 攻撃 .....	21, 167
EV-SSL 証明書 .....	134
GIGA スクール .....	61
GPS .....	66
https:// .....	132
ID とパスワードの漏えい .....	35
IoT 機器 .....	53
IoT 機器のセキュリティ .....	104
IPA .....	175, 181
NISC(内閣官房内閣サイバーセキュリティセンター) .....	28
OS .....	30
PIN コード .....	110
QR コード決済 .....	165
SECURITY ACTION .....	179
SMS 認証 .....	113
SNS .....	23, 58
VPN .....	130, 132

## あ行

アウトソーシング .....	155
アウトソース .....	151, 155, 181
アップデート .....	30
アプリのインストール .....	37
歩きスマホ .....	67
暗号化 .....	118, 124, 132, 138
暗号化処理 .....	99
暗号化メディア .....	144
暗号キー .....	112, 125, 145
暗号資産 .....	165
安否確認サービス .....	80
いいね! .....	60
位置情報 .....	66, 75, 77
位置情報共有アプリ .....	75
違法アップロード・ダウンロード .....	68
インターネットカフェ .....	87
ウェブサイトの改ざん .....	167
映像付き電話 .....	76
炎上 .....	62
お年寄り .....	76
オフショア開発 .....	160
オンライン決済 .....	165

## か行

海外でスマホやタブレットを活用する .....	88
画面ロック .....	40, 92
管理者 .....	153
キーロガー .....	87
機種変更 .....	96
帰宅マップ .....	83
キッズケータイ .....	75
共有設定 .....	156
クラウドストレージサービス .....	148
クラウドを活用 .....	152
クラッキング .....	70
クリエイティブ・コモンズ・ライセンス .....	170
警察庁サイバー犯罪対策プロジェクト .....	176
ゲームの不正行為 .....	69
公開範囲 .....	156
攻撃者 .....	15, 20, 50
攻撃を受けてしまったときの兆候と対処 .....	106
広告 .....	146
公衆無線 LAN .....	87, 94, 128, 147
個人情報 .....	60, 169
こども .....	74

## さ行

災害やテロに備えよう .....	80
サイバー攻撃 .....	14, 18, 50, 136, 158, 161
サイバーセキュリティ .....	28
サイバーセキュリティお助け隊サービス .....	180
サイバーセキュリティ関係法令Q&Aハンドブック .....	174
サイバーセキュリティ対策9か条 .....	28
サイバー犯罪 .....	72
サイバープロパガンダ .....	55
サプライチェーン攻撃 .....	160
ジオタグ .....	66
自撮り(セク스팅)被害 .....	24
事業継続計画(BCP) .....	152
辞書攻撃(ディクショナリアタック) .....	112
シャドーIT .....	154
常時SSL化 .....	134
肖像権 .....	171
情報収集 .....	81, 90, 159
情報モラル教育 .....	58, 168
情報流出 .....	19, 63, 148, 161
情報漏えい .....	41, 94, 97
証明書 .....	134
初期設定 .....	98

初期パスワード変更	105
人的損失	153
ストーカー	59
スパムメール	39
スマホ	31, 92
スマホ契約書	64
スマホのセキュリティ	92
スマホのセキュリティ対策プラン	93
成人年齢18歳引き下げ	73
生体認証	34, 98
セキュリティ資格	183
セキュリティソフト	30, 48
セキュリティ対策	150
ゼロデイ攻撃	56
総当たり攻撃(ブルートフォース攻撃)	111
相談窓口	45, 175
ソーシャルエンジニアリング	22
ソーシャルログイン	117
ソフトウェア	30

## た行

多要素認証	34, 113, 135
中間者攻撃	136
中小企業の情報セキュリティ対策ガイドライン	177
著作権	170
通知	92
データの暗号化	144
データローミング	87
データを消去する	101
デジタル遺産相続	78
デジタルタトゥー	59
デマ	71
テレワーク	154
電池をもたす	81
添付ファイル	39, 140
投資資金	151

## な行

ながらスマホ	67
なりすまし	24
偽サイト	36
偽メール	36
二段階認証	114
認知症の方の事故防止	77
認定情報処理支援機関(スマートSMEサポーター)	182
盗まれた情報	51
ネットいじめ	24, 59, 61
ネットワーク機器	31
ネットワークの設定	105

覗き見	44
乗っ取り	18, 50, 167

## は行

パクリ	68, 170
パスワード	32, 98, 110
パスワード使い回し	32
パスワードの保管・管理	33, 115, 120
パスワード流出チェック	121
パソコン	30
パソコンのセキュリティ	98
ハッカー	15
バックアップ	42, 95, 100, 153
犯罪勧誘	59
誹謗中傷対策	23
標的型メール	18, 39, 162
フィッシング	163
フェイクニュース	55
不正アクセス	164
不正送金	165
不正ログイン	166
負のコスト	150
プライバシー	69
プライバシーマーク	172
フリー素材	170
振り込め詐欺対策	76
紛失・盗難	44, 95, 102
ボットネット	52

## ま・や行

マイナンバーカード	185
マルウェア	16, 21, 53, 100, 140
身の安全を確保する	80
見守りメール	75
無線LAN	52, 124, 132
メール	138
メールアドレスの流出	142
メールアドレス流出チェック	121
誘拐・略取	24, 59

## ら行

ランサムウェア	18, 21, 43, 54, 166
リカバリメディア	98
リスト型攻撃(アカウントリスト攻撃・パスワードリスト攻撃)	112
リベンジポルノ	24, 59
リモートワイプ	99
リンク	39

下記の商標・登録商標をはじめ、本ハンドブックに記載されている会社名、システム名、製品名は一般に各社の商標または登録商標です。  
なお、本ハンドブックでは文中にて、TM、®は明記しておりません。

Adobe、Acrobat、Adobe ReaderはAdobe Systems Inc.の米国およびその他の国における商標または登録商標です。  
Firefoxは、Mozilla Foundationの米国およびその他の国における商標または登録商標です。  
Google、Android、Google Chromeは米国Google Inc.の米国およびその他の国における商標または登録商標です。  
iOSは、Apple Inc.の米国およびその他の国における商標または登録商標であり、ライセンスに基づき使用されています。  
Linuxは、Linus Torvalds氏の米国およびその他の国における商標または登録商標です。  
Macおよびmac OS、Safariは、Apple Inc.の米国および他の国における商標または登録商標です。  
Microsoft、Office、Word、Excel、PowerPointおよびWindowsは米国Microsoft Corporationの米国およびその他の国における商標または登録商標です。  
OracleとJavaは、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における商標または登録商標です。

内閣官房内閣サイバーセキュリティセンター (NISC)ウェブサイト：<https://www.nisc.go.jp/>  
NISC「みんなで使おうサイバーセキュリティ・ポータルサイト」：<https://security-portal.nisc.go.jp/>  
内閣サイバーセキュリティセンター 公式Twitter: @cas\_nisc  
内閣サイバー（注意・警戒情報）Twitter: @nisc\_forecast  
内閣サイバーセキュリティセンター NISC LINE公式アカウント：@nisc-forecast  
NISC Facebookページ: <https://www.facebook.com/nisc.jp>

## インターネットの安全・安心ハンドブック

2019年1月18日 Ver 4.00発行  
2020年3月31日 Ver.4.10発行  
2021年12月31日 Ver.4.20発行  
2023年1月31日 Ver.5.00発行



制作・著作 内閣官房 内閣サイバーセキュリティセンター (NISC)  
協力 警察庁 総務省 経済産業省 独立行政法人情報処理推進機構(IPA)  
改訂検討会メンバー：猪俣 敦夫（主査：大阪大学 教授）  
宮本 久仁男（株式会社NTT データシステム技術本部 サイバーセキュリティ技術部 情報セキュリティ推進室  
NTTDATA-CERT セキュリティマスター）  
松下 孝太郎（東京情報大学 総合情報学部 総合情報学科 教授）  
上沼 紫野（一般社団法人 虎ノ門南法律事務所 弁護士 安心ネットづくり促進協議会 理事）  
横山 尚人（独立行政法人情報処理推進機構（IPA） セキュリティセンター 企画部 エキスパート）  
酒井 啓悟（株式会社技術評論社 デジタル事業部）

インターネットの安全・安心ハンドブック（旧情報セキュリティハンドブック）は、サイバーセキュリティ普及・啓発に  
利用する限りにおいては多様な形で活用いただけます。

著作権は内閣サイバーセキュリティセンターが保有しますので、利用に際しては著作権者を表示してください。

クリエイティブコモンズライセンス 表示 - 非営利 - 継承 4.0 国際 (CC BY-NC-SA 4.0)

また、その際は、内閣サイバーセキュリティセンターウェブサイトのご意見・ご感想のメールアドレス（[security\\_awareness@cyber.go.jp](mailto:security_awareness@cyber.go.jp)）へ  
ご一報願います。

### 【活用例】

- PDF・コピー・製本の無料配布または印刷および作業実費での販売
- ページ単位・イラスト単位での利用
- 分割しての配布、必要部分だけを抜粋して配布
- 自団体のウェブサイトリンクを設置
- 表紙に使用する団体名を入れて利用
- 自団体のセキュリティ資料と合本して配布